MESURES p-ADIQUES

G. GRAS

Laboratoire de Mathématiques
U.A. 741 au C.N.R.S.
F–25030 Besançon Cedex

MESURES p-ADIQUES

par
Georges Gras

Cours du **DEA** 1990/1991 et
Publications Mathématiques de la
Faculté des Sciences de Besançon
(Théorie des Nombres)
Année 1991/1992

CHAPITRE 0

Introduction

Le but de ce cours est d'élaborer une théorie élémentaire de la mesure dans le cadre p-adique. Il nous faut donc, d'une part, préciser les objets sur lesquels seront définies des mesures, et, d'autre part, quel peut être le domaine des valeurs de ces mesures.

Le cadre naturel dans lequel la notion de mesure p-adique s'est imposée est celui des groupes de Galois issus de la théorie du corps de classes ; il s'agit donc de groupes profinis commutatifs particuliers ; la catégorie des groupes profinis abéliens constitue donc notre point de départ. D'un point de vue topologique, un résultat classique nous indique que ce sont exactement les groupes abéliens compacts totalement discontinus.

En ce qui concerne les valeurs prises par de telles mesures, si le cadre archimédien classique utilise $\mathbb{R}^+$, donc $\mathbb{R}$ ou $\mathbb{C}$ pour des mesures généralisées, il est ici naturel de remplacer le complété archimédien de $\mathbb{Q}$ par un complété p-adique, à savoir $\mathbb{Q}_p$, en vue des applications à l'arithmétique via l'analyse p-adique dans le corps $\mathbb{C}_p$ des "complexes p-adiques".

Si l'on a défini le clan $\mathcal{U}_G$ des parties mesurables d'un groupe profini G, au sens de la mesure μ, deux cas sont possibles a priori :

(i) $\{\mu(U),\, U \in \mathcal{U}_G\}$ est borné dans $\mathbb{Q}_p$; cet ensemble est donc contenu dans un disque de la forme $p^m\mathbb{Z}_p$, $m \in \mathbb{Z}$, auquel cas, quitte à normaliser autrement la mesure μ, on peut supposer qu'elle est à valeurs dans $\mathbb{Z}_p$; on dit alors que μ est une $\mathbb{Z}_p$-mesure sur G, ou plus simplement une mesure sur G ;

(ii) $\{\mu(U),\, U \in \mathcal{U}_G\}$ n'est pas borné ; nous montrerons que ce cas s'aborde assez facilement, au moins pour une catégorie particulière de telles "mesures" (que nous appellerons alors distributions) et qui s'expriment au moyen de "quotients" de $\mathbb{Z}_p$-mesures (au sens de (i)).

Rappelons que d'après J.-P. Serre [S1], la notion de mesure p-adique est dûe à B. Mazur, que les principales bases algébriques dont nous aurons besoin se trouvent déjà dans [S2] et que l'on trouve également un exposé différent de la théorie dans [L], [Ko] et [W], dans l'esprit des travaux d'Iwasawa [Iw] concernant la théorie des fonctions L p-adiques. Cependant nous reprendrons tous les arguments, même les plus élémentaires.

Les mesures p-adiques permettent évidemment d'exprimer tous les résultats classiques de façon plus concise mais leur principal intérêt est de mettre en évidence des liens structurels entre l'aspect analytique (représenté numériquement par les diverses intégrales par rapport à ces mesures) et l'aspect corps de classes (par l'intermédiaire du groupe de Galois G utilisé) ; en particulier, la seule connaissance des intégrales ne rend pas compte de certaines propriétés induites par la structure de G, ce qui nous a permis par exemple de trouver de nouvelles propriétés des fonctions L p-adiques (cf.[G1], [G2], [G3]).

Etant donné un groupe profini G, le clan $\mathcal{U}_G$ des parties "mesurables" doit donc vérifier les axiomes suivants :

(0.1) toute union finie d'éléments de $\mathcal{U}_G$ appartient à $\mathcal{U}_G$;

(0.2) le complémentaire d'un élément de $\mathcal{U}_G$ appartient à $\mathcal{U}_G$;

nous rajoutons la condition naturelle suivante :

(0.3) $G \in \mathcal{U}_G$;

il en résulte que toute intersection finie d'éléments de $\mathcal{U}_G$ appartient à $\mathcal{U}_G$.

Une $\mathbb{Z}_p$-mesure μ sur G est une application de $\mathcal{U}_G$ dans $\mathbb{Z}_p$ vérifiant l'axiome suivant d'additivité :

$$\text{(0.4)} \qquad \mu(U \cup V) = \mu(U) + \mu(V) \text{ pour tout } U, V \in \mathcal{U}_G,\ U \cap V = \emptyset.$$

Nous commencerons par illustrer ces définitions dans le cas d'un groupe commutatif fini G ; bien que relativement trivial, ce cas est indispensable car il est en un sens universel et conduit à introduire l'algèbre $\mathbb{Z}_p[G]$ du groupe G sur $\mathbb{Z}_p$ qui préfigure de façon essentielle les algèbres de $\mathbb{Z}_p$-mesures Λ_G lorsque G n'est pas fini. De plus, même lorsque G est infini, l'algèbre $\mathbb{Z}_p[G]$ apparaît comme une sous-algèbre dense de Λ_G pour la topologie naturelle qui sera définie sur Λ_G.

Si les chapitres I à IV ne contiennent aucun résultat nouveau à proprement parler, ils s'attachent à préparer la théorie des fonctions L p-adiques de $\mathbb{Q}$ (chapitre V) avec l'outil "distributions p-adiques" ; en outre nous justifions certains changements mineurs de définitions classiques concernant les nombres de Bernoulli (ordinaires et généralisés). Le chapitre V contient plusieurs améliorations de résultats classiques, des congruences nouvelles et les bases techniques permettant d'en obtenir d'autres.

CHAPITRE I

Algèbres de groupes – Limites projectives

1.— Les algèbres de groupes.

Soit R un anneau commutatif d'élément unité 1 et soit G un groupe arbitraire, noté multiplicativement, de neutre e.

Soit $R^{(G)}$ l'ensemble des applications de G dans R, à support fini, muni de la structure habituelle de R-module (*) ; en vue de ce qui va suivre, on note un élément de $R^{(G)}$ sous la forme symbolique :

$$\alpha = \sum_{g \in G} a_g g, \quad a_g \in R \text{ presque tous nuls ;} \tag{1.1}$$

ceci signifie simplement que $\alpha \in R^{(G)}$ est l'application qui à $g \in G$ associe $a_g \in R$, le support de α, noté $Supp(\alpha)$, étant fini. En pratique on écrit des sommes finies, les termes qui ne figurent pas correspondent à des coefficients nuls.

Au niveau de la structure de R-module on a donc, pour

$$\alpha = \sum_{g \in G} a_g g, \quad \beta = \sum_{g \in G} b_g g, \quad a_g, b_g \in R,$$

$$\alpha + \beta = \sum_{g \in G} (a_g + b_g) g, \tag{1.2}$$

$$a\alpha = \sum_{g \in G} (a a_g) g, \quad \text{pour tout } a \in R; \tag{1.3}$$

on a bien $Supp(\alpha + \beta)$ et $Supp(a\alpha)$ finis (i.e. $\alpha + \beta$, $a\alpha \in R^{(G)}$).

Le neutre de $R^{(G)}$ est noté 0.

Sur $R^{(G)}$ on définit un produit, dit produit de convolution :

Soient :

$$\alpha = \sum_{g \in G} a_g g, \beta = \sum_{g \in G} b_g g \in R^{(G)};$$

on pose :

$$\alpha\beta = \sum_{g \in G} c_g g, \; c_g = \sum_{h,k,hk=g} a_h b_k; \tag{1.4}$$

(*) A distinguer du R-module R^G des applications de G dans R ; on a $R^G = R^{(G)}$ si et seulement si G est fini.

la somme qui définit c_g a bien un sens dans R par finitude des supports de α et β ; en outre $Supp(\alpha\beta) \subseteq Supp(\alpha) \cup Supp(\beta)$ est bien fini et $\alpha\beta \in R^{(G)}$.

Il est élémentaire de vérifier que ce produit (1.4), joint aux lois de R-module (1.2), (1.3), confère à $R^{(G)}$ une structure de R-algèbre, que l'on note $R[G]$. On identifie le sous-anneau Re à R ; on identifie également $1.G$ à G qui est donc un sous-groupe de $(R[G])^*$, le groupe des inversibles de $R[G]$; enfin comme $1e$ est l'élément unité de $R[G]$ et que dans les identifications précédentes les trois neutres coïncident, on convient désormais de toujours noter 1 le neutre de G, l'unité de R, et par conséquent l'unité de $R[G]$.

(1.5) **Remarque.** (i) Il est clair que la R-algèbre $R[G]$ est commutative si et seulement si G est commutatif, ce que nous supposerons au niveau de la théorie de la mesure.

(ii) La R-algèbre $R[G]$ est R-libre de base (dite base canonique) formée des éléments de G.

(1.6) **Exemple.** Si $R = \mathbb{Z}$ et $G = \{1, \sigma, \sigma^2\}$ (groupe cyclique d'ordre 3 engendré par σ), tout élément de $\mathbb{Z}[G]$ s'écrit

$$\alpha = a + b\sigma + c\sigma^2,\ a, b, c \in \mathbb{Z},$$

et on a par exemple le calcul suivant dans $\mathbb{Z}[G]$:

$$(1 - \sigma)(1 + \sigma + \sigma^2) = 1 + \sigma + \sigma^2 - \sigma - \sigma^2 - 1 = 0.$$

2.— Mesures sur un groupe abélien fini – Intégration.

Soit G un groupe abélien fini ; il est clair que $\mathcal{U}_G = \mathcal{P}(G)$, l'ensemble des parties de G , vérifie les axiomes (0.1) à (0.3), et qu'une $\mathbb{Z}_p$-mesure μ est définie de façon unique, par les valeurs $\mu(\{g\}) \in \mathbb{Z}_p$, $g \in G$, puisque l'on a alors, d'après l'axiome (0.4) :

$$\mu(U) = \sum_{g \in U} \mu(\{g\}), \text{ pour tout } U \in \mathcal{U}_G.$$

Si à μ on associe

$$\alpha = \sum_{g \in G} \mu(\{g\})g \in \mathbb{Z}_p[G]\ ,$$

on voit que l'ensemble des $\mathbb{Z}_p$-mesures sur G est en correspondance bijective avec $\mathbb{Z}_p[G]$; pour cette raison, nous convenons de confondre les notations μ et α et nous disons, par abus, que $\mu \in \mathbb{Z}_p[G]$ *est* une $\mathbb{Z}_p$-mesure sur G ; on écrit alors

$$\mu(\{g\}) = \mu(g),$$

auquel cas μ s'écrit

$$\mu = \sum_{g \in G} \mu(g)g,$$

et pour toute partie U de G, sa mesure est $\mu(U) = \sum_{g \in U}\ \mu(g)$.

(2.1) **Remarque.** On peut définir, a priori, une structure de $\mathbb{Z}_p$-algèbre sur l'ensemble $\mathcal{M}_G$ des mesures (somme de mesures, multiplication scalaire, produit de convolution) ; on constate alors que la correspondance précédente est un isomorphisme de $\mathbb{Z}_p$-algèbres. Ceci sera fait dans le cas général plus loin (cf. chap.II, §2) et ne présente aucune difficulté.

(2.2) **Intégration des fonctions p-adiques sur G fini.** Une application de G dans $\mathbb{C}_p$ est donc (cf. §1) un élément du $\mathbb{C}_p$-espace vectoriel $\mathbb{C}_p^G$; on peut toujours munir $\mathbb{C}_p^G$ du produit de convolution (*) (et non du produit usuel défini par $(f_1 f_2)(g) = f_1(g) f_2(g)$ pour tout $g \in G$), ce qui fait que l'on peut alors voir les fonctions sur G comme les éléments de $\mathbb{C}_p[G]$. Bien entendu on peut être amené à considérer aussi le produit usuel sur $\mathbb{C}_p^G$ (ce sera le cas des caractères de G). On utilisera à cet effet les notations $\mathbb{C}_p^G$ ou $\mathbb{C}_p[G]$ pour indiquer la structure envisagée.

Soit alors $f \in \mathbb{C}_p^G$; si μ est une mesure sur G , l'intégrale

$$\int_G f d\mu$$

est ici une intégrale discrète qui ne peut se définir que par la somme

$$\langle f, \mu \rangle = \sum_{g \in G} f(g)\mu(g).$$

(2.2.1) **Cas des caractères.** Toujours dans le cas où G est abélien fini, on peut introduire le groupe X_G des caractères de G à valeurs dans $\mathbb{C}_p^\times$; ce groupe s'identifie à une partie de $\mathbb{C}_p^G$ mais ne constitue pas un sous-monoïde multiplicatif de $\mathbb{C}_p[G]$ car X_G est muni du produit usuel et non du produit de convolution (si χ, $\psi \in X_G$, il leur correspond, dans $\mathbb{C}_p[G]$, $f_\chi = \sum_{g \in G} \chi(g)g$, $f_\psi = \sum_{g \in G} \psi(g)g$, pour lesquels on a $f_\chi f_\psi = 0$ si $\chi \neq \psi$ et $f_\chi^2 = |G| f_\chi$ sinon, alors que $\chi\psi$ correspond à $\sum_{g \in G}(\chi(g)\psi(g))g$).

Si $\chi \in X_G$ et si $\mu \in \mathbb{Z}_p[G]$, on peut considérer l'intégrale correspondante pour la fonction χ et la mesure μ :

$$\langle \chi, \mu \rangle = \sum_{g \in G} \chi(g)\mu(g);$$

on a alors le résultat suivant :

(2.2.2) **Proposition.** Soient λ, $\mu \in \mathbb{Z}_p[G]$ et soit $\chi \in X_G$; alors on a :
(i) $\langle \chi, \lambda + \mu \rangle = \langle \chi, \lambda \rangle + \langle \chi, \mu \rangle$;
(ii) $\langle \chi, a\lambda \rangle = a\langle \chi, \lambda \rangle$, pour tout $a \in \mathbb{Z}_p$;
(iii) $\langle \chi, \lambda\mu \rangle = \langle \chi, \lambda \rangle \langle \chi, \mu \rangle$.

Ceci résulte immédiatement du fait que χ est un homomorphisme de G dans $\mathbb{C}_p^\times$ et qu'il se prolonge , de façon unique, en un homomorphisme de $\mathbb{Z}_p$-algèbres de $\mathbb{Z}_p[G]$ dans $\mathbb{C}_p$. Pour cette raison, $\langle \chi, \mu \rangle$ se note aussi $\chi(\mu)$.

(*) car ici, G étant fini, on a $\mathbb{C}_p^G = \mathbb{C}_p^{(G)}$.

(2.3) **Transformée de Fourier discrète.** Soit toujours G un groupe abélien fini. Soit $f \in \mathbb{C}_p[G]$ vue comme fonction sur G à valeurs dans $\mathbb{C}_p$. Si $\chi \in X_G$ et si $f = \sum_{\sigma \in G} f(\sigma)\sigma$, on pose $\chi(f) = \sum_{\sigma \in G} f(\sigma)\chi(\sigma)$.

(2.3.1) **Définition.** On appelle transformée de Fourier discrète de f la famille

$$(\chi(f))_{\chi \in X_G} \in \mathbb{C}_p^{|G|}.$$

L'application

$$\Phi : \mathbb{C}_p[G] \longrightarrow \mathbb{C}_p^{|G|}$$

qui à f associe $(\chi(f))_\chi$ est un homomorphisme de $\mathbb{C}_p$-algèbres (*) appelé la transformation de Fourier discrète sur $\mathbb{C}_p[G]$.

(2.3.2) **Proposition.** La transformée de Fourier Φ est bijective et la transformée inverse Φ^{-1} est donnée, pour $\alpha = (\alpha_\chi)_\chi \in \mathbb{C}_p^{|G|}$, par

$$\Phi^{-1}(\alpha) = \sum_{\chi \in X_G} \alpha_\chi e_\chi, \text{ où } e_\chi = \frac{1}{|G|} \sum_{\tau \in G} \chi(\tau^{-1})\tau.$$

On vérifie que $(e_\chi)_{\chi \in X_G}$ constitue un système fondamental d'idempotents orthogonaux de $\mathbb{C}_p[G]$, à savoir que l'on a :

(i) $1 = \sum_{\chi \in X_G} e_\chi$,

(ii) $e_\chi e_\psi = 0$ si $\chi \neq \psi$,

ce qui implique :

(iii) $e_\chi^2 = e_\chi$ pour tout $\chi \in X_G$.

Par conséquent, ces propriétés conduisent à la décomposition

$$\mathbb{C}_p[G] = \bigoplus_{\chi \in X_G} \mathbb{C}_p[G]e_\chi$$

(somme directe d'idéaux de $\mathbb{C}_p[G]$). D'après (iii), chaque $\mathbb{C}_p[G]e_\chi$ est une $\mathbb{C}_p$-algèbre unitaire d'élément unité e_χ , et l'application

$$\begin{aligned} \mathbb{C}_p[G] &\longrightarrow \prod_{\chi \in X_G} \mathbb{C}_p[G]e_\chi \\ f &\longrightarrow (fe_\chi)_\chi \end{aligned}$$

est alors un isomorphisme de $\mathbb{C}_p[G]$-algèbres unitaires ; il ne reste plus qu'à identifier $\mathbb{C}_p[G]e_\chi$ et calculer fe_χ :

Pour tout $\sigma \in G$, on a

$$\sigma e_\chi = \frac{1}{|G|} \sum_{\tau \in G} \chi(\tau^{-1})\sigma\tau = \frac{1}{|G|} \sum_{s \in G} \chi(\sigma s^{-1})s = \frac{1}{|G|}\chi(\sigma) \sum_{s \in G} \chi(s^{-1})s = \chi(\sigma)e_\chi;$$

(*) où $\mathbb{C}_p^{|G|}$ est la $\mathbb{C}_p$-algèbre produit direct de $|\ G\ |$ exemplaires de $\mathbb{C}_p$.

donc $fe_\chi = \sum_{\sigma\in G} f(\sigma)\sigma e_\chi = \Big(\sum_{\sigma\in G} f(\sigma)\chi(\sigma)\Big)e_\chi = \chi(f)e_\chi$; autrement dit $\mathbb{C}_p[G]e_\chi \simeq \mathbb{C}_p e_\chi$, et finalement l'application

$$\Phi_\chi : \mathbb{C}_p[G]e_\chi \longrightarrow \mathbb{C}_p,$$

qui à fe_χ associe $\chi(f)$, est un isomorphisme de $\mathbb{C}_p$-algèbres unitaires (donc de corps).

La transformée de Fourier Φ est donc l'isomorphisme :

$$\begin{aligned} \mathbb{C}_p[G] = \bigoplus_{\chi\in X_G} \mathbb{C}_p[G]e_\chi &\xrightarrow{\oplus\Phi_\chi} \mathbb{C}_p^{|G|} \\ f &\longrightarrow \big(\chi(f)\big)_\chi \end{aligned} \tag{2.3.3}$$

et la transformée inverse est bien celle indiquée.

(2.3.4) **Corollaire.** Si $f \in \mathbb{C}_p[G]$, on a :

$$f = \frac{1}{|G|}\sum_{\chi\in X_G} \chi^{-1}(f)\chi,$$

qui montre que toute fonction sur G est combinaison $\mathbb{C}_p$-linéaire de caractères de G.

On a $f = \Phi^{-1}\circ\Phi(f) = \sum_{\chi\in X_G}\chi(f)e_\chi$, soit

$$\begin{aligned} f &= \sum_\chi \chi(f)\frac{1}{|G|}\sum_\sigma \chi^{-1}(\sigma)\sigma \\ &= \frac{1}{|G|}\sum_\sigma \sigma\sum_\chi \chi(f)\chi^{-1}(\sigma), \end{aligned}$$

qui donne, par identification, si l'on pose $f = \sum_\sigma f(\sigma)\sigma$:

$$\begin{aligned} f(\sigma) &= \frac{1}{|G|}\sum_\chi \chi(f)\chi^{-1}(\sigma) \\ &= \frac{1}{|G|}\sum_\chi \chi^{-1}(f)\chi(\sigma), \end{aligned}$$

ou encore :

$$f = \frac{1}{|G|}\sum_{\chi\in X_G}\chi^{-1}(f)\chi.$$

(2.3.5) **Corollaire.** Un élément f de $\mathbb{C}_p[G]$ est non nul et non diviseur de 0 dans cette algèbre si et seulement si $\chi(f) \neq 0$ pour tout $\chi \in X_G$.

Ceci résulte de l'isomorphisme (2.3.3).

(2.3.6) **Remarque.** La transformée de Fourier discrète justifie le fait que l'on utilise le produit de convolution et non le produit usuel. Compte-tenu de ce qui a été dit en (2.2.1) au sujet des caractères, l'identité (2.3.4) a lieu dans $\mathbb{C}_p^G$ et non dans $\mathbb{C}_p[G]$. On remarque aussi que l'inclusion $\mathbb{Z}_p[G] \subset \mathbb{C}_p[G]$ permet d'envisager la transformée de Fourier d'une $\mathbb{Z}_p$-mesure μ.

3.— Limites projectives de groupes et anneaux topologiques.

Nous aurons à utiliser des limites projectives de groupes et anneaux commutatifs, munis d'une topologie. Commençons par le cas des groupes, le cas des anneaux étant analogue.

Soit I un ensemble d'indices, ordonné, supposé filtrant à droite ; ceci signifie que si $i, j \in I$ alors il existe $k \in I$ tel que l'on ait $k \geq i$ et $k \geq j$.

(3.1) **Définitions.** a) On dit que l'on a un système projectif de groupes si l'on s'est donné :

(i) une famille de groupes G_i , indexée par I filtrant à droite,

(ii) une famille d'homomorphismes de groupes (dits de transition) $h_{ij} : G_i \to G_j$, indexée par l'ensemble des $(i, j) \in I \times I$ tels que $i \geq j$, vérifiant les conditions suivantes :

(α) h_{ii} est l'identité sur G_i pour tout $i \in I$;

(β) $h_{ik} = h_{jk} \circ h_{ij}$ chaque fois que $i, j, k \in I$ vérifient $i \geq j \geq k$;

autrement dit on a les diagrammes commutatifs suivants (pour $i \geq j \geq k$) :

$$\begin{array}{ccc} & G_j & \\ h_{ij} \nearrow & & \searrow h_{jk} \\ G_i & \xrightarrow{h_{ik}} & G_k \end{array}$$

Un tel système est noté (G_i, h_{ij}).

b) On appelle limite projective du système projectif (G_i, h_{ij}) le sous-groupe

$$\varprojlim_{i \in I} G_i$$

du groupe produit $\prod_{i \in I} G_i$, formé des familles $(g_i)_{i \in I}$ (dites cohérentes) qui vérifient la condition suivante :

$$g_j = h_{ij}(g_i) \text{ pour tout } i, j \in I \text{ tels que } i \geq j.$$

(3.2) **Remarques.** (i) Le fait que $\varprojlim_{i \in I} G_i$ soit un sous-groupe de $\prod_{i \in I} G_i$ se vérifie immédiatement et utilise complètement le fait que les h_{ij} sont des homomorphismes de groupes ;

(ii) dans le diagramme caractérisant la condition (β), la condition de cohérence $h_{ik}(g_i) = g_k$ est impliquée par les 2 autres ($g_k = h_{jk}(g_j)$, $g_j = h_{ij}(g_i)$);

(iii) la notation $\varprojlim_{i \in I} G_i$ est relative au système des h_{ij} qui est en général canonique par rapport à la famille $(G_i)_{i \in I}$, et donc souvent non précisé. De même lorsque I est implicite, on abrège en écrivant $\varprojlim G_i$.

(3.3) **Définitions.** (i) Si les groupes G_i sont des groupes topologiques on adjoint aux définitions (3.1) précédentes la condition que les homomorphismes de transition h_{ij} sont

continus. Le groupe $\varprojlim_{i\in I} G_i$ est alors muni de la topologie induite par la topologie produit sur $\prod_{i\in I} G_i$; un système fondamental de voisinages du neutre dans $\varprojlim G_i$ est formé des

$$V_J = \left(\prod_{i\in J} V_i \times \prod_{i\in I-J} G_i\right) \bigcap \varprojlim_{i\in I} G_i,$$

où $J \subset I$ est fini et où, pour i fixé, V_i parcourt un système fondamental de voisinages du neutre de G_i.

(ii) On dit que $G = \varprojlim_{i\in I} G_i$ est un groupe profini si les G_i sont finis pour tout $i \in I$ et munis de la topologie discrète. Si de plus les G_i sont cycliques, on dit que G est procyclique.

(3.4) **Homomorphismes de systèmes projectifs de groupes.** On suppose donnés deux systèmes projectifs de groupes (G_i, h_{ij}) et (G'_i, h'_{ij}) indexés par le même ensemble I. Supposons qu'il existe un système d'homomorphismes de groupes :

$$f_i : G_i \to G'_i,\ i \in I,$$

tels que l'on ait, pour tout $i, j \in I$, $i \geq j$, les diagrammes commutatifs suivants :

$$\begin{array}{ccc} G_i & \xrightarrow{f_i} & G'_i \\ h_{ij}\downarrow & & \downarrow h'_{ij} \\ G_j & \xrightarrow{f_j} & G'_j \end{array} \qquad (3.4.1)$$

on peut alors créer l'application :

$$f : \varprojlim G_i \longrightarrow \varprojlim G'_i \qquad (3.4.2)$$

définie par $f((g_i)_i) = (f_i(g_i))_i$, dont on vérifie qu'elle est un homomorphisme de groupes de $\varprojlim G_i$ dans $\varprojlim G'_i$ (la commutativité des diagrammes ci-dessus étant nécessaire pour que la famille des $f_i(g_i)$ soit cohérente).

Si les f_i sont des isomorphismes, on vérifie que f est un isomorphisme de $\varprojlim G_i$ sur $\varprojlim G'_i$.

On dit alors que f est un homomorphisme (resp. isomorphisme) de systèmes projectifs (de groupes).

En ce qui concerne les limites projectives d'anneaux (topologiques ou non) les définitions sont analogues :

Etant donnés les anneaux A_i d'éléments unités 1_i, $i \in I$, et les homomorphismes d'anneaux $h_{ij} : A_i \to A_j$, pour tout $i, j \in I$, $i \geq j$, vérifiant les conditions $(\alpha), (\beta)$ de (3.1), $\varprojlim_{i\in I} A_i$ est donc le sous-anneau de $\prod_{i\in I} A_i$ formé des familles cohérentes.

On rappelle que pour la structure d'anneaux, les homomorphismes respectent les éléments unités, auquel cas on a $h_{ij}(1_i) = 1_j$ pour tout $i \geq j$, et l'élément $(1_i)_{i\in I}$ est l'élément unité de $\varprojlim A_i$.

On remarque enfin qu'il y a cohérence au niveau des définitions de limites projectives de groupes et anneaux, autrement dit que le groupe additif sous-jacent de l'anneau $\varprojlim A_i$ est bien la limite projective des groupes additifs des A_i.

(3.5) **Parties cofinales.** Soit $J \subseteq I$ vérifiant les conditions suivantes :
(i) pour tout $j \in J$ il existe $i \in I$ tel que $i \geq j$,
(ii) pour tout $i \in I$ il existe $j \in J$ tel que $j \geq i$;
on dit que J est cofinale par rapport à I.

Soit alors (A_i, h_{ij}) un système projectif (d'anneaux par exemple) indexé par I ; on vérifie que J est filtrant à droite et donc que $\varprojlim_{j\in J} A_j$ existe. On a alors le résultat suivant (énoncé ici pour la structure d'anneaux) :

(3.5.1) **Proposition.** Si $J \subseteq I$ est cofinale par rapport à I, on a $\varprojlim_{i\in I} A_i \simeq \varprojlim_{j\in J} A_j$ (algébriquement et topologiquement).

A l'élément $x = (x_i)_{i\in I} \in \varprojlim_{i\in I} A_i$ associons $x' = (x_j)_{j\in J}$; on vérifie que $x' \in \varprojlim_{j\in J} A_j$ et que cette application est un homomorphisme d'anneaux. Si $x' = 0$, on a $x_j = 0$ pour tout $j \in J$; or si $i \in I$, il existe $j \in J$ tel que $j \geq i$, et on a donc $h_{ij}(x_j) = x_i$; d'où $x_i = h_{ij}(0) = 0$; d'où $x = 0$ et l'injectivité.

Soit $x' = (x_j)_{j\in J} \in \varprojlim_{j\in J} A_j$. Soit $i \in I$; par hypothèse il existe $j \in J$, $j \geq i$; posons alors $x_i = h_{ji}(x_j)$. On crée ainsi une famille $(x_i)_{i\in I}$, dont on vérifie la cohérence, qui est un antécédent de x'. D'où l'isomorphisme. On vérifie alors la bicontinuité.

(3.5.2) **Remarque.** C'est cette propriété qui justifie le mieux l'idée de limite, dans la mesure où une partie cofinale J conduit chaque fois à une "suite extraite" qui représente le même élément limite.

Par exemple, lorsque l'ensemble d'indices est $\mathbb{N}$, muni de son ordre total habituel, toute partie infinie de $\mathbb{N}$ est cofinale à $\mathbb{N}$.

(3.6) **Exemples.** (i) On considère $I = \mathbb{N}$ muni de son ordre naturel et $A_n = \mathbb{Z}/p^n\mathbb{Z}$ pour tout $n \in I$, muni de la topologie discrète, où p est un nombre premier fixé ; pour $m \geq n$ on définit les homomorphismes de transition :

$$h_{m,n} : A_m \to A_n,$$

par $h_{m,n}(a + p^m\mathbb{Z}) = a + p^n\mathbb{Z}$, pour tout $a \in \mathbb{Z}$. On obtient alors

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

qui n'est autre que l'anneau des entiers p-adiques $\mathbb{Z}_p$, comme on peut le vérifier de la façon suivante si l'on a construit $\mathbb{Z}_p$ comme $\{x \in \mathbb{Q}_p, |x|_p \leq 1\}$, $\mathbb{Q}_p$ étant par définition

une complétion de $\mathbb{Q}$ pour la valeur absolue p-adique $|\ |_p$: à $x \in \mathbb{Z}_p$, x donné par son développement de Hensel $x = \sum_{i \geq 0} a_i p^i$, $a_i \in \{0, 1, \ldots, p-1\}$, on associe $\left(\sum_{i=0}^{n-1} a_i p^i + p^n \mathbb{Z}\right)_n$.

(ii) On considère $I = \mathbb{N} - \{0\}$ muni cette fois de l'ordre défini par la relation de divisibilité dans $\mathbb{Z}$, et $A_n = \mathbb{Z}/n\mathbb{Z}$ pour tout $n \in I$, muni de la topologie discrète ; pour n divisant m, on définit :

$$h_{m,n} : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

par $h_{m,n}(a + m\mathbb{Z}) = a + n\mathbb{Z}$, pour tout $a \in \mathbb{Z}$.

L'anneau $\varprojlim \mathbb{Z}/n\mathbb{Z}$ ainsi obtenu s'appelle le complété profini de $\mathbb{Z}$ et se note $\widehat{\mathbb{Z}}$.

(3.6.1) **Remarques.** (i) En utilisant le théorème des restes chinois convenablement, on vérifie que l'on a l'homéomorphisme :

$$\widehat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p,$$

où p parcourt l'ensemble des nombres premiers (ceci sera retrouvé en (III.2.3)).

(ii) Dans les exemples précédents, on vérifie que l'homéomorphisme d'anneaux $\mathbb{Z}_p \simeq \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ conduit à celui des groupes multiplicatifs :

$$\mathbb{Z}_p^* \simeq \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^*,$$

et de même $\widehat{\mathbb{Z}} \simeq \varprojlim \mathbb{Z}/n\mathbb{Z} \simeq \prod_p \mathbb{Z}_p$ conduit à

$$\widehat{\mathbb{Z}}^* \simeq \varprojlim (\mathbb{Z}/n\mathbb{Z})^* \simeq \prod_p \mathbb{Z}_p^*.$$

(3.7) **Théorie de Galois infinie.** Il s'agit de l'exemple essentiel pour nous : soit K/k une extension algébrique galoisienne et soit $\mathcal{F}$ la famille des sous-extensions galoisiennes finies F/k de K/k ; on sait que

$$K = \bigcup_{F \in \mathcal{F}} F.$$

Soit $G = Gal(K/k)$ (i.e. le groupe des k-automorphismes de K), et pour tout $F \in \mathcal{F}$ posons $G_F = Gal(F/k)$. Si l'on ordonne $\mathcal{F}$ par inclusion et si l'on définit, pour $F, F' \in \mathcal{F}$, $F' \subseteq F$,

$$h_{F,F'} : G_F \longrightarrow G_{F'}$$

comme étant l'homomorphisme de restriction des k-automorphismes de F à F' (ou la projection $G/Gal(K/F) \simeq G_F \longrightarrow G/Gal(K/F') \simeq G_{F'}$) il n'est pas difficile de montrer que l'on a

$$G \simeq \varprojlim_{F \in \mathcal{F}} G_F,$$

relativement au système projectif ci-dessus défini :

De façon précise, si à $\sigma \in G$ on associe la famille de ses restrictions $(\sigma_F)_{F\in\mathcal{F}}$ on définit évidemment un homomorphisme de G dans $\varprojlim G_F$ (la cohérence résultant de l'existence même de σ) ; cet homomorphisme est injectif car si $\sigma_F = id_F$, pour tout $F \in \mathcal{F}$, pour $x \in K$ et F contenant x, on a $\sigma(x) = \sigma_F(x) = x$. Il est enfin surjectif : si $(\sigma_F)_{F\in\mathcal{F}} \in \varprojlim G_F$ montrons qu'il suffit de poser, pour tout $x \in K$, $\sigma(x) = \sigma_F(x)$ dès que F contient x ; pour cela on vérifie que $\sigma(x)$ ne dépend pas du choix de F contenant x, ensuite que σ est un k-automorphisme de K (i.e. $\sigma \in G$), et enfin que les restrictions de σ à F sont les σ_F, pour tout $F \in \mathcal{F}$.

En pratique on identifie G et $\varprojlim_{F\in\mathcal{F}} G_F$.

(3.7.1) **Remarque**. On notera qu'en général une extension galoisienne infinie K/k peut s'écrire comme réunion d'extensions finies particulières qui constituent une partie cofinale par rapport à $\mathcal{F}$; par exemple, si $k = \mathbb{Q}$ et si K est l'extension abélienne maximale $\mathbb{Q}^{ab}$ de $\mathbb{Q}$, le "corps de classes" sur $\mathbb{Q}$ montre que la famille des corps cyclotomiques $\mathbb{Q}(m)$, des racines m-ièmes de l'unité, $m \geq 1$, constitue une partie cofinale (*) par rapport à $\mathcal{F}$ qui permet d'identifier très facilement $Gal(\mathbb{Q}^{ab}/\mathbb{Q})$ (cf. chap. IV).

(3.7.2) **Corollaire**. En utilisant la théorie des corps finis, on déduit qu'une clôture algébrique $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$ a pour groupe de Galois $\widehat{\mathbb{Z}}$.

(3.7.3) **Remarque**. La correspondance de Galois, dans le cas infini, suppose que l'on munisse $Gal(K/k)$ de la topologie de groupe profini définie en (3.3) ; nous renvoyons le lecteur aux références classiques détaillant ces questions, comme [Ri], en rappelant simplement que cette correspondance de Galois associe (de façon bijective décroissante) les sous-extensions L (finies ou non) de K/k et les sous-groupes *fermés* H de G ; on a alors $L = K^H$ et $H = Gal(K/L)$.

(3.8) **Propriété universelle des limites projectives**. Bien que cet aspect ne nous soit pas essentiel, signalons que la notion de limite projective résoud le problème universel suivant :

Soit (A_i, h_{ij}) un système projectif (d'anneaux par exemple) indexé par I ; alors il existe un anneau A et une famille d'homomorphismes $f_i : A \to A_i$, $i \in I$, tels que les diagrammes suivants soient commutatifs pour tout $i, j \in I$, $i \geq j$:

$$\begin{array}{ccc} A_i & \xrightarrow{h_{ij}} & A_j \\ & {\scriptstyle f_i}\nwarrow \quad \nearrow{\scriptstyle f_j} & \\ & A & \end{array}$$

(*) Le point (très difficile) montrant cette cofinalité est, de façon précise, le "théorème de Kronecker-Weber" disant que toute extension abélienne finie de $\mathbb{Q}$ est contenue dans un corps cyclotomique.

Si $(A', (f_i')_{i\in I})$ est une autre solution, alors il existe un unique isomorphisme $u : A' \to A$, rendant commutatifs les diagrammes suivants, pour tout $i \in I$:

$$\begin{array}{ccc} A' & \xrightarrow{u} & A \\ & f_i' \searrow \quad \swarrow f_i & \\ & A_i & \end{array}$$

Il suffit de poser $A = \varprojlim_{i\in I} A_i$ et de prendre pour f_i les restrictions à A des projections $\prod_{k\in I} A_k \longrightarrow A_i$.

Pour l'unicité, on remarque qu'il faut prendre pour u l'application $A' \xrightarrow{\prod f_k'} \prod_{k\in I} A_k$ dont l'image est dans A.

4.— Topologie des limites projectives de groupes ou anneaux compacts.

Soit (A_i, h_{ij}) un système projectif d'anneaux topologiques indexé par I; on suppose les anneaux A_i compacts pour tout $i \in I$. De ce fait le produit $\prod_{i\in I} A_i$ est compact et le fait que $A = \varprojlim_{i\in I} A_i$ soit lui-même compact résulte de la propriété plus générale suivante (valable évidemment pour la seule structure de groupe) :

(4.1) **Proposition**. La limite projective d'anneaux séparés est un sous-anneau fermé du produit direct de ces anneaux.

Montrons, lorsqu'il est non vide, que le complémentaire de $\varprojlim A_i$ est ouvert : Soit $a \notin \varprojlim A_i$; ceci signifie que $a = (a_i)_{i\in I}$ n'est pas cohérente, donc qu'il existe $i, j \in I$, $i \geq j$, tels que $h_{i,j}(a_i) \neq a_j$; séparons a_j et $h_{ij}(a_i)$ par des voisinages V_j et W dans A_j ; comme par définition $h_{ij} : A_i \to A_j$ est continu, il existe un voisinage V_i de a_i dans A_i tel que $h_{ij}(V_i) \subseteq W$; considérons le voisinage $V = \prod_{k\in I-\{i,j\}} A_k \times V_i \times V_j$ de a dans $\prod_{i\in I} A_i$; alors $V \cap \varprojlim A_i = \emptyset$ car aucun élément de V ne peut être cohérent, l'obstruction venant des facteurs V_i, V_j puisque $h_{ij}(V_i) \cap V_j = \emptyset$. D'où le résultat.

Remarquons que dans le cas où les A_i sont discrets on peut prendre $V_i = \{a_i\}$, $V_j = \{a_j\}$ $(W = \{h_{ij}(a_i)\})$, auquel cas la non cohérence dans V est encore plus radicale.

(4.1.1) **Corollaire**. Tout groupe profini est compact.

Nous allons maintenant approfondir le cas des groupes profinis.

L'énoncé suivant permet de caractériser l'ensemble des sous-groupes ouverts d'un groupe compact G :

(4.2) **Proposition**. Soit G un groupe compact. Il a alors les propriétés suivantes :

(i) Tout sous-groupe ouvert de G est compact ;

(ii) un sous-groupe H de G est ouvert si et seulement si il est d'indice fini dans G.

Dans un groupe topologique, tout sous-groupe ouvert est fermé ; d'où (i).

Si H est un sous-groupe ouvert de G et si les g_iH, $i \in I$, sont les classes distinctes de G modulo H, elles constituent une partition du compact G formée d'ouverts ; d'où la finitude de I. Inversement, si H est d'indice fini dans G, le groupe G/H est fini et compact (l'application canonique $q : G \to G/H$ étant continue par définition), donc discret, auquel cas H, image réciproque par q du neutre de G/H, est en particulier ouvert.

(4.3) **Notation.** Si G est un groupe topologique compact (par exemple un groupe profini), nous désignons par Ω_G l'ensemble des sous-groupes ouverts (i.e. d'indice fini) de G.

A partir de maintenant, nous ne considérons, comme groupes compacts, que des groupes profinis (commutatifs).

On a le résultat suivant qui caractérise les groupes profinis de façon exclusivement topologique :

(4.4) **Théorème.** Les conditions suivantes sont équivalentes :

(i) G est un groupe profini ;

(ii) G est un groupe compact dans lequel l'ensemble Ω_G des sous-groupes ouverts constitue un système fondamental de voisinages de 1 ;

(iii) G est un groupe compact totalement discontinu.

démonstration

(i) $\Rightarrow$ (ii). La compacité résulte d'un cas particulier de (4.1) dans le cas des groupes.

Ecrivons $G = \varprojlim_{i \in I} G_i$, où les G_i sont des groupes finis notés multiplicativement ; par définition de la topologie produit, un système fondamental de voisinages de 1 dans $\prod_{i \in I} G_i$ est formé des sous-groupes ouverts :

$$V_J = \prod_{i \in I-J} G_i \times \prod_{j \in J} \{1_j\},\ J \subseteq I,\ J \text{ fini} ;$$

par conséquent, les sous-groupes $V_J \cap G$ forment un système fondamental de voisinages ouverts de 1 dans G et sont dans Ω_G.

(ii) $\Rightarrow$ (iii). Soit C la composante connexe de 1 dans G ; c'est un sous-groupe de G (en effet , par translation par g^{-1}, pour $g \in C$, $g^{-1}C$, qui est connexe et qui contient 1, est égale à C ; d'où $C^{-1}C \subseteq C$). Par conséquent, pour tout $H \in \Omega_G$, $C \cap H$ est un sous-groupe ouvert et fermé non vide de C, d'où $C \cap H = C$, soit $C = \cap_{H \in \Omega_G}(C \cap H) = C \cap \cap_{H \in \Omega_G} H = C \cap \{1\} = \{1\}$.

(iii) $\Rightarrow$ (i). D'après un résultat général classique sur la connexité (cf. [Bo, ch.II, pp. 224–225]) les voisinages ouverts fermés de 1 constituent un système fondamental de voisinages (ils sont donc ouverts compacts).

Soit alors V un tel voisinage ; comme V et $G - V$ sont compacts et disjoints, on peut les séparer en ce sens qu'il existe un voisinage ouvert symétrique W de 1 tel que $WV \cap W(G - V) = \emptyset$; on a donc $WV \subseteq V$. Par récurrence sur $n \geq 0$, on vérifie que $W^n \subseteq V$ et donc que le sous-groupe L de G engendré par W, $L = \cup_{n \geq 0} W^n$, est contenu dans V ; comme c'est un ouvert, on a $L \in \Omega_G$ et $L \subseteq V$. D'où $\cap_{H \in \Omega_G} H = \{1\}$.

On en déduit alors que l'application canonique $G \longrightarrow \prod_{H \in \Omega_G} G/H$, qui à $g \in G$ associe $(gH)_H$, induit un homomorphisme de groupes injectif f de G dans $\varprojlim_{H \in \Omega_G} G/H$

(Ω_G étant ordonné par l'ordre opposé à l'inclusion, les homomorphismes de transition $h_{K,H}$, $H, K \in \Omega_G$, $K \subseteq H$, étant les projections canoniques $G/K \to G/H$).

(4.4.1) **Lemme.** Cet homomorphisme f est surjectif.

Soit $(g_H H)_H$, $g_H \in G$, un élément de $\varprojlim G/H$, et considérons la famille des g_H ; si on a H, K, $L \in \Omega_G$, K, $L \subseteq H$, on a $g_K H = g_L H$ par cohérence, et donc $g_K g_L^{-1} \in H$; on a donc une suite de Cauchy qui converge puisque G est compact donc complet ; si $g \in G$ est la limite, on a, pour tout $H \in \Omega_G$, l'existence de $K \in \Omega_G$, $K \subseteq H$ (i.e. K assez petit) tel que $g g_H^{-1} \in K$, soit $gK = g_H K$, ce qui conduit à $gH = g_H H$, ce qu'il fallait établir.

On vérifie enfin que f est bicontinue.

Ceci montre l'implication (iii) $\Rightarrow$ (i) puisqu'alors les G/H sont finis discrets.

(4.4.2) **Remarque.** On obtient en particulier que tout groupe profini "abstrait" se retrouve, comme limite projective de groupes finis, au moyen de l'homéomorphisme canonique :

$$G \simeq \varprojlim_{H \in \Omega_G} G/H.$$

(4.5) **Corollaire.** Tout sous-groupe fermé K d'un groupe profini commutatif G est profini.

En effet, il suffit de considérer (iii).

5.— Sous-groupes de Sylow d'un groupe profini commutatif.

(5.1) **Ordre généralisé d'un élément.** Soit $G = \varprojlim_{i \in I} G_i$ un groupe profini commutatif indexé par I, et soit $g \in G$, $g = (g_i)_{i \in I}$, $g_i \in G_i$; on peut donner un sens à la notion d'ordre de g, cet ordre étant un produit symbolique $\prod_p p^{n_p}$, où p parcourt l'ensemble $\mathbb{P}$ des nombres premiers, et où $n_p \in \mathbb{N} \cup \{\infty\}$. Ceci se conçoit dans la mesure où, lorsque $i, j \in I$, $i \geq j$, la relation $h_{ij}(g_i) = g_j$ montre que l'ordre (au sens ordinaire) de g_i est un multiple de celui de g_j ; en particulier, si l'on désigne par $p^{n_p^i}$, $n_p^i \geq 0$, la p-partie de l'ordre de g_i, pour tout $p \in \mathbb{P}$, on a les relations $n_p^i \geq n_p^j$, pour tout i, $j \in I$ tels que $i \geq j$; par conséquent comme I est filtrant à droite, il est naturel de poser $n_p = Sup_{i \in I}(n_p^i)$ dans $\mathbb{N} \cup \{\infty\}$, il est clair que l'on a le fait suivant :

L'élément $g \in G$ est d'ordre fini si et seulement si on a $n_p = 0$ pour presque tout $p \in \mathbb{P}$ et $n_p < \infty$ pour tout $p \in \mathbb{P}$; lorsque c'est le cas, l'entier $\prod_p p^{n_p}$ est l'ordre au sens usuel de g. En particulier, il y a 2 façons (non exclusives) pour g d'être d'ordre infini :

(i) on a $n_p \neq 0$ pour une infinité de $p \in \mathbb{P}$,

(ii) on a $n_p = \infty$ pour au moins $p \in \mathbb{P}$.

(5.1.1) **Définition.** On appelle ordre (généralisé) de $g \in G$ le produit formel $\prod_{p \in \mathbb{P}} p^{n_p}$, noté $o(g)$. On munit l'ensemble de ces produits formels d'une structure évidente de monoïde multiplicatif (contenant $\mathbb{N} - \{0\}$ comme sous-monoïde) dans lequel les notions de divisibilité, p.g.c.d., p.p.c.m., sont immédiates.

(5.1.2) **Remarque.** Introduisons les supports $S_0 = \{p \in \mathbb{P}, 0 < n_p < \infty\}$, $S_\infty = \{p \in \mathbb{P}, n_p = \infty\}$; alors S_0 et S_∞ peuvent être indépendamment vides, finis non vides ou infinis

(utiliser $\widehat{\mathbb{Z}}^*$ en remarquant que dans $\widehat{\mathbb{Z}}^*$, tout élément $\neq 1$ de $1 + 2p\mathbb{Z}_p \simeq \mathbb{Z}_p$ est d'ordre p^∞).

(5.1.3) **Indices généralisés.** Soit H un sous-groupe fermé du groupe profini commutatif G. On vérifie que, de façon analogue, on peut définir l'indice généralisé $(G : H)$ en posant $(G : H) = p.p.c.m.((G/U : H/(H \cap U)))$, lorsque U parcourt Ω_G. On a en particulier l'ordre généralisé $\mid G \mid$ de G. L'ordre généralisé $\mid H \mid$ de H existe aussi puisque H est profini. On vérifie facilement que toutes les propriétés élémentaires des ordres et indices de sous-groupes dans le cas $\mid G \mid$ fini ont lieu ici pour les ordres des éléments et les indices des sous-groupes fermés (cf. [S2]), à ceci près que p^∞/p^∞ n'est pas défini.

(5.2) **Sous-groupes de Sylow.** On appelle p-Sylow du groupe profini commutatif G le sous-groupe $G(p) = \{g \in G,\ o(g)$ divise $p^\infty\}$; si $g = (g_i)_{i \in I}$, $g \in G(p)$ si et seulement si les g_i sont tels que $o(g_i)$ est une puissance (finie) de p. On vérifie que $G(p)$ est un sous-groupe fermé de G ; son ordre $\mid G(p) \mid$ est donc une puissance finie ou non de p.

(5.3) **Remarque.** On notera que la notion d'ordre d'un élément est un peu plus précise que celle d'ordre d'un sous-groupe fermé dans la mesure où l'on a $\mid \mathbb{Z}_p^n \mid = p^\infty$ quel que soit $n \geq 1$, tandis que dans $G = \mathbb{Z}_p^n$ on pourra définir des éléments $\gamma_1, \ldots, \gamma_n$, d'ordres respectifs p^∞, et qui "engendrent " G.

Nous reviendrons sur ces questions dans le chapitre III (cf. §2) lorsque nous aurons besoin de décomposer un groupe profini en ses p-Sylow.

CHAPITRE II

Algèbre des mesures p-adiques

On fixe, dans ce chapitre, un nombre premier p et on se donne un groupe profini commutatif G de neutre 1. On rappelle que l'ensemble Ω_G des sous-groupes ouverts (i.e. d'indice fini) de G est un système fondamental de voisinages de 1 (cf. (I.4.4)).

1.— Clan des parties mesurables de G.

On rappelle que, d'après l'introduction, on souhaite définir un clan $\mathcal{U}_G$ de parties de G satisfaisant aux axiomes (0.1) à (0.3) ; de plus, tout $H \in \Omega_G$ étant lui-même un groupe profini tel que $G = \bigcup gH$ (réunion finie), il est naturel de souhaiter que $\mathcal{U}_G$ contienne l'ensemble $\mathcal{C}_G$ des classes de G modulo les éléments de Ω_G. On a le résultat suivant :

(1.1) **Proposition.** Tout ouvert compact U de G est réunion finie disjointe d'éléments de $\mathcal{C}_G$ et même de classes modulo H pour $H \in \Omega_G$ convenable.

En effet, en tout $g \in U$ soit $H_g \in \Omega_G$ tel que $gH_g \subseteq U$; on a donc $U = \cup_{g \in U} gH_g$ et par compacité de U il existe un recouvrement fini de U de la forme $\cup_{i=1}^{n} g_i H_{g_i}$, $g_i \in G$. On pose alors $H = \bigcap_{i=1}^{n} H_i$, où $H_i = H_{g_i}$; comme les H_i sont d'indice fini dans G, il en est de même pour H ; on a aussi $H_i = \cup_{j=1}^{n_i} h_{ij} H$, $h_{ij} \in H_i$, d'où $U = \cup_{i=1}^{n} \cup_{j=1}^{n_i} g_i h_{ij} H$.

Ceci invite à poser la définition suivante :

(1.2) **Définition.** On désigne par $\mathcal{U}_G$ l'ensemble des ouverts compacts de G (i.e. l'ensemble des réunions finies de classes modulo un élément de Ω_G) et on appelle $\mathbb{Z}_p$- mesure sur G toute application $\mu : \mathcal{U}_G \to \mathbb{Z}_p$ satisfaisant à la condition d'additivité (0.4).

(1.3) **Remarques.** (i) Il est clair que $\mathcal{U}_G$ satisfait aux axiomes (0.1) à (0.3) et qu'il contient $\mathcal{C}_G$.

(ii) La définition ne peut s'étendre aux ouverts non fermés de G car par exemple si les complémentaires des points étaient mesurables, les parties $\{g\}$, $g \in G$, le seraient aussi, ce qui ne peut se concevoir si G est infini. Par ailleurs, le choix du clan $\mathcal{U}_G$ est très conforme à l'idée de mesure puisque en tout $g \in G$, $\mathcal{U}_G$ contient un système fondamental de voisinages de g.

(iii) Les sous-groupes fermés H non ouverts (i.e. non d'indice fini dans G) ne sont pas mesurables.

Nous allons vérifier que toute mesure est caractérisée par sa restriction à l'ensemble $\mathcal{C}_G$ des classes gH, $g \in G$, $H \in \Omega_G$.

(1.4) **Proposition.** Soit μ_0 une application de $\mathcal{C}_G$ dans $\mathbb{Z}_p$ satisfaisant à la condition suivante :
pour tout H, $K \in \Omega_G$, $K \subseteq H$, on a :

$$(1.4.1) \qquad \mu_0(gH) = \sum_{hK \in H/K} \mu_0(ghK), \text{ pour tout } g \in G. \ (*)$$

(*) La sommation porte sur les classes de H modulo K (notées hK pour un représentant h non précisé) et non sur l'indice h.

Alors il existe une mesure μ et une seule sur G dont la restriction à $\mathcal{C}_G$ soit μ_0.

(1.5) **Corollaire.** L'ensemble des $\mathbb{Z}_p$-mesures sur G s'identifie à l'ensemble des applications de $\mathcal{C}_G$ dans $\mathbb{Z}_p$ vérifiant la condition de cohérence (1.4.1).

Il est clair que toute mesure μ conduit aux relations de cohérence (1.4.1), par additivité finie.

Soit $\mu_0 : \mathcal{C}_G \to \mathbb{Z}_p$ vérifiant (1.4.1), et soit $U \in \mathcal{U}_G$; montrons que pour toute écriture de U sous la forme d'une réunion disjointe finie (cf. (1.1)) :

$$U = \bigcup_i a_i H,\ a_i \in G,\ H \in \Omega_G,$$

la somme $\sum_i \mu_0(a_i H)$ est constante :

Supposons avoir également $U = \cup_j b_j K$, $b_j \in G$, $K \in \Omega_G$ (réunion finie disjointe), et soit $L = H \cap K$; on a

$$H = \bigcup_u h_u L,\ K = \bigcup_v k_v L,\ h_u \in H,\ k_v \in K$$

(réunions finies disjointes), d'où les 2 partitions finies suivantes de U :

$$U = \bigcup_i \bigcup_u a_i h_u L = \bigcup_j \bigcup_v b_j k_v L. \tag{1.5.1}$$

Par application de (1.4.1) il vient :

$$\mu_0(a_i H) = \sum_u \mu_0(a_i h_u L) \text{ et } \sum_i \mu_0(a_i H) = \sum_i \sum_u \mu_0(a_i h_u L)\ ;$$

de même, $\sum_j \mu_0(b_j K) = \sum_j \sum_v \mu_0(b_j k_v L)$, d'où l'égalité de ces sommes d'après (1.5.1), compte-tenu de l'unicité de la décomposition de U en classes modulo L disjointes, ce qui permet de définir $\mu(U)$ sans ambiguité.

Il reste à vérifier qu'une telle fonction μ est bien additive :

Soient $U, V \in \mathcal{U}_G$ tels que $U \cap V = \emptyset$. Quitte à choisir $H \in \Omega_G$ assez petit, on peut supposer que

$$U = \bigcup_{i \in I} g_i H,\ V = \bigcup_{j \in J} g_j H \quad \text{(réunions finies disjointes)},$$

auquel cas $\mu(U \cup V) = \sum_{k \in I \cup J} \mu_0(g_k H)$ par définition, d'où

$$\mu(U \cup V) = \sum_{i \in I} \mu_0(g_i H) + \sum_{j \in J} \mu_0(g_j H) = \mu(U) + \mu(V).$$

(1.6) **Remarque.** Par abus de notation, nous confondons μ et sa restriction μ_0 à $\mathcal{C}_G$ et appelons $\mathbb{Z}_p$-mesure sur G toute fonction sur $\mathcal{C}_G$ vérifiant la condition de cohérence (1.4.1), étant entendu que la mesure de tout $U \in \mathcal{U}_G$ s'obtient par la formule :

$$\mu(U) = \sum_i \mu(g_i H), \tag{1.6.1}$$

pour n'importe quelle partition finie $U = \cup_i g_i H$, $g_i \in G$, pour $H \in \Omega_G$ assez petit (comparer au cas G fini en (I, §2)).

2.— Algèbre des $\mathbb{Z}_p$-mesures.

Nous commençons par une approche naïve (qui peut être omise sans inconvénient) des définitions, avant d'établir le résultat fondamental du §3 qui s'appuie sur ceux du §1.

(2.1) **Définitions.** Soit $\mathcal{M}_G$ l'ensemble des $\mathbb{Z}_p$-mesures sur G (au sens de (1.6)). On munit canoniquement $\mathcal{M}_G$ d'une structure de $\mathbb{Z}_p$-module en définissant $\lambda + \mu$ et $a\lambda$, pour λ, $\mu \in \mathcal{M}_G$, $a \in \mathbb{Z}_p$, de la façon suivante (sur $\mathcal{C}_G$) :

(i) $(\lambda + \mu)(gH) = \lambda(gH) + \mu(gH)$, pour tout $g \in G$, $H \in \Omega_G$;

(ii) $(a\lambda)(gH) = a\lambda(gH)$, pour tout $g \in G$, $H \in \Omega_G$;

puis on définit le produit de convolution de la façon suivante :

$$\text{(iii)}\ (\lambda\mu)(gH) = \sum_{\substack{aH,bH \in G/H \\ abH = gH}} \lambda(aH)\mu(bH), \text{ pour tout } g \in G,\ H \in \Omega_G.$$

(2.2) **Remarque.** La formule (iii) résulte de l'écriture multiplicative de G ; elle est à comparer à une écriture additive de la forme

$$(\lambda\mu)(x) = \sum_{t+s=x} \lambda(t)\mu(s) = \sum_t \lambda(t)\mu(x-t).$$

Si les définitions (i) et (ii) donnent de façon évidente des mesures, la définition (iii) demande une vérification de la relation de cohérence (1.4.1) :

Soient K, $H \in \Omega_G$, $K \subseteq H$; posons $H = \cup_{hK \in H/K}\ hK$. On a

$$(\lambda\mu)(gH) = \sum_{\substack{aH,bH \in G/H \\ abH = gH}} \lambda(aH)\mu(bH)\ ;$$

décomposons aH et bH sous la forme $\cup_u\ uK$, $\cup_v\ vK$, u, $v \in G$ tels que $uH = aH$, $vH = bH$; la condition $abH = gH$ est équivalente à $uvH = gH$, soit $uvK \in \{ghK,\ hK \in H/K\}$; on a donc

$$(\lambda\mu)(gH) = \sum_{\substack{aH,bH \in G/H \\ abH = gH}} \lambda(\bigcup_u\ uK)\ \mu(\bigcup_v\ vK),$$

ce qui donne, par additivité de λ et μ,

$$\begin{aligned}(\lambda\mu)(gH) &= \sum_{\substack{aH,bH\in G/H\\ abH=gH}} \sum_{\substack{uK,vK\\ uH=aH,vH=bH}} \lambda(uK)\mu(vK)\\ &= \sum_{\substack{uK,vK\\ uvK\in gH/K}} \lambda(uK)\mu(vK)\\ &= \sum_{hK\in H/K} \sum_{\substack{uK,vK\\ uvK=gH/K}} \lambda(uK)\mu(vK)\\ &= \sum_{hK\in H/K} \mu(ghK)\end{aligned}$$

par définition.

D'où le résultat.

(2.3) **Remarque.** Considérons la $\mathbb{Z}_p$-algèbre $\mathcal{A}(\mathcal{C}_G, \mathbb{Z}_p)$ des applications de $\mathcal{C}_G$ dans $\mathbb{Z}_p$, munie de la topologie de la convergence ponctuelle ; comme $\mathbb{Z}_p$ est compact, cette algèbre est compacte. Pour voir que $\mathcal{M}_G$ est compacte, il suffit d'établir qu'elle est fermée dans $\mathcal{A}(\mathcal{C}_G, \mathbb{Z}_p)$, ce qui s'établit en remarquant que $\mathcal{M}_G$ est une intersection d'images réciproques de la forme

$$f_{g,H,K}^{-1}(\{0\}),\ g \in G,\ H, \in \Omega_G, \quad K \subseteq H,$$

où $f_{g,H,K}$ est l'application (continue) qui à $\alpha \in \mathcal{A}(\mathcal{C}_G, \mathbb{Z}_p)$ associe $\alpha(gH) - \sum_{hK\in H/K} \alpha(gh\ K) \in \mathbb{Z}_p$.

Nous allons voir que cette définition "fonctionnelle" de $\mathcal{M}_G$ peut être remplacée par un formalisme beaucoup plus agréable pour les applications à l'arithmétique et qui nous rapproche du cas G fini (cf. (I. §2)).

3.— Définition algébrique de l'algèbre des $\mathbb{Z}_p$-mesures.

On a le résultat suivant (qui peut servir de définition de $\mathcal{M}_G$) :

(3.1) **Théorème.** Soit G un groupe profini commutatif et soit $\mathcal{M}_G$ la $\mathbb{Z}_p$-algèbre des mesures sur G (cf. (2.1), (2.3)). Alors $\mathcal{M}_G$ est homéomorphe à la $\mathbb{Z}_p$-algèbre $\Lambda_G = \varprojlim_H \mathbb{Z}_p[G/H]$ où H parcourt l'ensemble Ω_G des sous-groupes ouverts de G, muni de l'ordre opposé à l'inclusion, et où les homomorphismes de transition $h_{K,H}$, pour $K \subseteq H$, sont les prolongements par $\mathbb{Z}_p$-linéarité des applications canoniques $G/K \to G/H$.

démonstration

Soit $\mu \in \mathcal{M}_G$; c'est donc une application de $\mathcal{C}_G$ dans $\mathbb{Z}_p$ telle que $\mu(gH) = \sum_{hK\in H/K} \mu(ghK)$, pour tout $g \in G$, $H, K \in \Omega_G$, $K \subseteq H$ (cf. (1.4)).

Posons alors, pour tout $H \in \Omega_G$:

$$\mu_H = \sum_{gH\in G/H} \mu(gH)gH \in \mathbb{Z}_p[G/H].$$

Soit $K \in \Omega_G$ tel que $K \subseteq H$ et calculons $h_{K,H}(\mu_K) = \sum_{gK \in G/K} \mu(gK)gH$; décomposons g sous la forme ah, $aH \in G/H$, $hK \in H/K$; il vient :

$$\sum_{gK \in G/K} \mu(gK)gH = \sum_{aH \in G/H} \sum_{hK \in H/K} \mu(ahK)\, aH$$
$$= \sum_{aH \in G/H} \mu(aH)\, aH,$$

par additivité de μ ; d'où $h_{K,H}(\mu_K) = \mu_H$ comme attendu.

On a donc $(\mu_H)_H \in \varprojlim_H \mathbb{Z}_p[G/H]$, et on vérifie que l'application $\mu \longrightarrow (\mu_H)_H$ est un homomorphisme bijectif de $\mathbb{Z}_p$-modules.

En ce qui concerne la structure d'anneaux, soient λ, $\mu \in \mathcal{M}_G$ et considérons $\lambda\mu$. On a

$$(\lambda\mu)_H = \sum_{gH \in G/H} (\lambda\mu)(gH)\, gH$$
$$= \sum_{gH \in G/H} \sum_{\substack{aH,bH \in G/H \\ abH = gH}} \lambda(aH)\mu(bH)\, gH$$
$$= \sum_{aH,bH \in G/H} \lambda(aH)\mu(bH)\, aH\ bH$$
$$= \lambda_H\, \mu_H \quad \text{dans } \mathbb{Z}_p[G/H]\ .$$

D'où un isomorphisme de $\mathbb{Z}_p$-algèbres pour lequel il reste à établir la bicontinuité.

Pour cela examinons la topologie de Λ_G. D'après (I.4.1), c'est une algèbre compacte puisque les $\mathbb{Z}_p[G/H] \simeq \mathbb{Z}_p^{(G:H)}$ (comme $\mathbb{Z}_p$-modules) sont compacts. Un système fondamental de voisinages de 0 dans Λ_G est donc formé des traces sur Λ_G des idéaux suivants de $\prod_{H \in \Omega_G} \mathbb{Z}_p[G/H]$:

$$V_{\Omega,\,n} = \prod_{H \in \Omega_G - \Omega} \mathbb{Z}_p[G/H] \times \prod_{H \in \Omega} p^n \mathbb{Z}_p[G/H], \tag{3.1.1}$$

où les $\Omega \subset \Omega_G$ sont finis et où $n \in \mathbb{N}$.

Il suffit alors d'utiliser (2.3) pour arriver facilement au résultat.

(3.1.2) **Remarque**. Si l'on considère l'algèbre $\mathbb{Z}_p[G]$ (cf. (I, §1)), l'application

$$\mathbb{Z}_p[G] \longrightarrow \Lambda_G$$
$$\sum_g a_g\, g \longrightarrow \left(\sum_g a_g\, gH\right)_H$$

est une injection qui permet d'identifier $\mathbb{Z}_p[G]$ à une sous-algèbre de Λ_G ; on a alors le résultat suivant :

(3.2) **Proposition**. La $\mathbb{Z}_p$-algèbre $\mathbb{Z}_p[G]$ est dense dans Λ_G.

En effet, soit $V_{\Omega,n}$ l'un des voisinages définis en (3.1.1). Comme Ω est fini, $K = \cap_{H\in\Omega} H$ est un élément de Ω_G pour lequel μ_K se projette sur μ_H, pour tout $H \in \Omega$ puisque $K \subseteq H$; donc si $\mu_K = \sum_{gK\in G/K} \mu(gK)\ gK$, le relèvement $\mu' = \sum_{gK\in G/K} \mu(gK)\ g$, est un relèvement dans $\mathbb{Z}_p[G]$ qui est tel que $\mu - \mu' \in V_{\Omega,n}$ (pour tout n en fait), comme on le vérifie facilement par projection sur les $\mathbb{Z}_p[G/H]$, $H \in \Omega$ (i.e. $H \supseteq K$).

(3.3) **Remarque**. Si G est fini, on a $\{1\} \in \Omega_G$, auquel cas $\Lambda_G = \varprojlim_H \mathbb{Z}_p[G/H]$ s'identifie canoniquement à $\mathbb{Z}_p[G]$. Par contre, si G est infini, on vérifie que $\mathbb{Z}_p[G]$ est distincte de Λ_G.

(3.4) **Conclusion**. Pour "voir" une mesure $\mu \in \Lambda_G = \varprojlim \mathbb{Z}_p[G/H]$, il suffit de considérer, pour H "assez petit" (i.e. G/H "assez gros"), la composante μ_H de μ sur $\mathbb{Z}_p[G/H]$: elle s'écrit $\mu_H = \sum_{gH\in G/H} \mu(gH)\ gH$ et, pour chaque classe gH, le coefficient de gH est par définition la mesure de la classe gH. Si on a un ouvert compact U, on sait qu'il existe un tel H pour lequel $U = \cup_{i=1}^n g_iH$ (réunion finie disjointe) auquel cas $\mu(U) = \sum_{i=1}^n \mu(g_iH)$ se déduit des coefficients de μ_H (on se ramène en quelque sorte au cas fini du chapitre I). En outre

$$\mu' = \sum_{gH\in G/H} \mu(gH)\ g$$

est une mesure qui approche μ dans Λ_G (ce relèvement dépend du choix des représentants g des classes modulo H ; on vérifie facilement que deux tels relèvements diffèrent d'un élément de l'idéal d'augmentation de H dans $\mathbb{Z}_p[G]$, i.e. l'idéal de $\mathbb{Z}_p[G]$ engendré par les $1 - h$, $h \in H$).

4.— Mesures particulières.

(4.1) **Mesures de Dirac**. Soit $g \in G$; considéré comme élément de $\mathbb{Z}_p[G] \subseteq \Lambda_G$, il définit une mesure μ qui est donc telle que $\mu_H = gH$ pour tout $H \in \Omega_G$; autrement dit :

$$\begin{aligned} &\mu(aH) = 0 \quad \text{si } aH \neq gH, \\ &\mu(gH) = 1 \quad \text{sinon .} \end{aligned}$$

Cette mesure s'appelle la mesure de Dirac en g et se note encore g.

Un élément de $\mathbb{Z}_p[G]$ est donc une combinaison $\mathbb{Z}_p$-linéaire de mesures de Dirac (et leur ensemble est donc dense dans Λ_G).

(4.2) **Mesures invariantes par translation**. Comme dans le cadre classique, on s'intéresse aux mesures μ telles que (G étant multiplicatif) :

$$g\mu = \mu, \quad \text{pour tout } g \in G. \tag{4.2.1}$$

Dans $\mathbb{Z}_p[G/H]$, $H \in \Omega_G$, la relation (4.2.1) conduit à

$$(1 - gH)\mu_H = 0, \quad \text{soit}$$

$$(1-gH)\sum_{aH\in G/H}\mu(aH)\,aH=0\ ;$$

notons pour simplifier σ, $\tau,\ldots$ les éléments gH, aH de G/H ; il vient

$$(1-\sigma)\sum_{\tau\in G/H}\mu(\tau)\,\tau=0\quad\text{pour tout }\sigma\in G/H.$$

On a donc $\sum_\tau(\mu(\tau)-\mu(\tau\sigma^{-1}))\tau=0$, soit $\mu(\tau\sigma^{-1})=\mu(\tau)$ pour tout σ, $\tau\in G/H$; d'où $\mu(\tau)=c_H\in\mathbb{Z}_p$, c_H indépendant de τ, et on obtient :

$$\mu_H=c_H\sum_{\tau\in G/H}\tau. \tag{4.2.2}$$

Par cohérence, $\mu(G)$ s'obtient en projetant (4.2.2) dans $\mathbb{Z}_p[G/G]=\mathbb{Z}_p$, à partir de n'importe quel H, ce qui donne

$$\mu(G)=c_H\sum_{\tau\in G/H}1,$$

soit

$$\mu(G)=c_H(G:H),\quad\text{pour tout } H\in\Omega_G,\quad\text{avec } c_H\in\mathbb{Z}_p. \tag{4.2.3}$$

Introduisons alors le p-Sylow $G(p)$ de G (cf. (I, §5)) qui peut s'écrire (cf. (I.5.2.2)) :

$$G(p)=\varprojlim_H(G/H)(p)\ :$$

(i) Si $G(p)$ est infini, on peut donc trouver une suite de $H_n\in\Omega_G$ pour lesquels $(G:H_n)=p^n$, $n\in\mathbb{N}$; donc par (4.2.3) on a $\mu(G)=c_{H_n}\,p^n$, et, puisque $c_{H_n}\in\mathbb{Z}_p$, $\mu(G)=0$, et $c_H=0$ pour tout $H\in\Omega_G$; d'où $\mu=0$ (cf. (4.2.2)).

(ii) Si $G(p)$ est fini, il existe $H_0\in\Omega_G$ tel que $G/H_0\simeq G(p)$, auquel cas on a, d'après (4.2.3),

$$\mu(G)=c_{H_0}\mid G(p)\mid,$$

qui montre que, si μ existe, la mesure de G est un $\mathbb{Z}_p$-multiple de $\mid G(p)\mid$. On peut alors écrire (cf. (4.2.2), (4.2.3)) :

$$\begin{aligned}\mu_H&=\frac{\mu(G)}{(G:H)}\sum_{gH\in G/H}gH\\&=\frac{c_{H_0}\mid G(p)\mid}{(G:H)}\sum_{gH\in G/H}gH,\quad\text{pour tout } H\in\Omega_G;\end{aligned} \tag{4.2.4}$$

or $\frac{|G(p)|}{(G:H)}\in\mathbb{Z}_p$ pour tout H, ce qui fait que l'on a $\mu_H\in\mathbb{Z}_p[G/H]$ pour tout $H\in\Omega_G$; enfin comme $(\mu_H)_H$ est dans $\varprojlim_H\mathbb{Z}_p[G/H]$, il existe dans ce cas des mesures invariantes

par translation et en fait une seule, à normalisation près, que nous appellerons la mesure de Haar sur G :

(4.3) **Théorème**. Soit G un groupe profini commutatif. Si le p-Sylow $G(p)$ de G est infini la seule $\mathbb{Z}_p$-mesure de G invariante par translation est la mesure nulle. Si $G(p)$ est fini, toute $\mathbb{Z}_p$-mesure de G invariante par translation est donnée par $\mu = c\alpha_G$, $c \in \mathbb{Z}_p$, où α_G est la mesure de Haar définie par

$$\alpha_G = \left(\frac{\mid G(p) \mid}{(G:H)} \sum_{gH \in G/H} gH \right)_{H \in \Omega_G},$$

et pour laquelle $\alpha_G(G) = \mid G(p) \mid$.

(4.4) **Corollaire**. Si G est fini, on a simplement

$$\alpha_G = \frac{\mid G(p) \mid}{\mid G \mid} \sum_{g \in G} g.$$

(4.5) **Remarque**. Dans le cas où $G(p)$ est infini, pour tout $c \in \mathbb{Z}_p - \{0\}$, la famille $\left(\frac{c}{(G:H)} \sum_{gH \in G/H} gH\right)_H$ définit un élément de $\varprojlim \mathbb{Q}_p[G/H]$ qui serait donc du ressort des "mesures " non bornées évoquées dans l'Introduction. Nous verrons plus tard ce qu'il en est ; notamment, contrairement au vocabulaire utilisé dans [Ko] et [W], on ne peut appeler cet élément une "mesure de Haar" .

(4.6) **Proposition**. Si G est somme directe de 2 sous-groupes profinis G_1 et G_2, dont les p-Sylow sont finis, on a $\alpha_G = \alpha_{G_1}\ \alpha_{G_2}$.

En effet, prenons pour décrire $\varprojlim_H \mathbb{Z}_p[G/H]$, $H \in \Omega_G$, la partie cofinale des $H = H_1 \oplus H_2$, où $H_i \in \Omega_{G_i}$, $i = 1, 2$.
On a alors :

$$\frac{\mid G(p) \mid}{(G:H)} \sum_{gH \in G/H} gH = \frac{\mid G_1(p) \mid\mid G_2(p) \mid}{(G_1 : H_1)(G_2 : H_2)} \sum_{g_1 H_1,\, g_2 H_2} g_1 g_2 (H_1 \oplus H_2)$$

$$= \frac{\mid G_1(p) \mid}{(G_1 : H_1)} \sum_{g_1 H_1 \in G_1/H_1} g_1 H_1 . \frac{G_2(p)}{(G_2 : H_2)} \sum_{g_2 H_2 \in G_2/H_2} g_2 H_2,$$

qui définit $\alpha_{G_1}\ \alpha_{G_2}$ dans $\varprojlim \mathbb{Z}_p[G/H] = \Lambda_G$.

5.— Intégration par rapport à une $\mathbb{Z}_p$-mesure.

(5.1) **Définition de $\int_G f d\mu$**. Soit f une application continue de G dans $\mathbb{C}_p$; comme G est compact, pour tout ε réel strictement positif il existe $H_\varepsilon = H \in \Omega_G$ et une fonction f_ε, constante sur chaque classe gH (i.e. localement constante modulo H), tels que :

$$(5.1.1) \qquad \mid f - f_\varepsilon \mid_p = \sup_{x \in G} \{ \mid f(x) - f_\varepsilon(x) \mid_p \} \leq \varepsilon,$$

où $|\ |_p$ est la valeur absolue habituelle sur $\mathbb{C}_p$ (normalisée par la condition $|\ p\ |_p = \frac{1}{p}$). Soit $\mu \in \Lambda_G$; si $\mu_H = \sum_{gH \in G/H} \mu(gH)\ gH$, pour le groupe H ci-dessus, on pose :

$$\int_G f_\varepsilon(x)\ d\mu(x) = \sum_{gH \in G/H} \mu(gH)\ f_\varepsilon(gH), \tag{5.1.2}$$

où $f_\varepsilon(gH) = f_\varepsilon(y)$ pour n'importe quel $y \in gH$.

Notons $\langle f_\varepsilon, \mu_H \rangle$ le second membre de (5.1.2) (cf. (I, §2)) et montrons qu'il ne dépend pas du choix de H tel que f_ε soit localement constante modulo H :

Si $K \in \Omega_G$ est un autre sous-groupe pour lequel f_ε est localement constante modulo K, posons $L = H \cap K$ et comparons $\langle f_\varepsilon, \mu_H \rangle$ et $\langle f_\varepsilon, \mu_K \rangle$; en vertu des relations de cohérence définissant μ, il vient, puisque f_ε est a fortiori localement constante modulo L :

$$\begin{aligned} \langle f_\varepsilon, \mu_H \rangle &= \sum_{aL \in G/L} \mu(aL)\ f_\varepsilon(aL) = \langle f_\varepsilon, \mu_L \rangle, \\ \langle f_\varepsilon, \mu_K \rangle &= \sum_{aL \in G/L} \mu(aL)\ f_\varepsilon(aL) = \langle f_\varepsilon, \mu_L \rangle, \end{aligned} \tag{5.1.3}$$

ce qui fait que $\langle f_\varepsilon, \mu_H \rangle$ ne dépend que de f_ε et peut se noter $\langle f_\varepsilon, \mu \rangle$ (et définit en quelque sorte la notion d'intégrale pour les "fonctions en escalier", étant entendu qu'ici les partitions utilisées sont les classes modulo H, $H \in \Omega_G$, pour H assez petit).

Il reste alors à voir que les $\langle f_\varepsilon, \mu \rangle$ ont une limite indépendante du choix de la famille $(f_\varepsilon)_\varepsilon$ satisfaisant (5.1.1) lorsque $\varepsilon \to 0$:

Pour cela comparons $\langle f_\varepsilon', \mu \rangle$ et $\langle f_{\varepsilon'}', \mu \rangle$ où f_ε' (resp. $f_{\varepsilon'}'$) sont 2 fonctions localement constantes modulo $H = H_\varepsilon$ (resp. $H' = H_{\varepsilon'}$), telles que $|\ f - f_\varepsilon'\ |_p < \varepsilon$ (resp. $|\ f - f_{\varepsilon'}'\ |_p < \varepsilon'$) ; il suffit de prendre $L = H \cap H'$ pour constater que

$$\begin{aligned} |\ \langle f_\varepsilon', \mu \rangle - \langle f_{\varepsilon'}', \mu \rangle\ |_p &= |\ \langle f_\varepsilon', \mu_L \rangle - \langle f_{\varepsilon'}', \mu_L \rangle\ |_p \quad \text{(d'après (5.1.3))} \\ &= |\ \sum_{gL \in G/L} \mu(gL)(f_\varepsilon'(gL) - f_{\varepsilon'}'(gL))\ |_p \\ &\leq \operatorname*{Max}_{gL \in G/L} |\ f_\varepsilon'(gL) - f_{\varepsilon'}'(gL)\ |_p \\ &\leq \operatorname*{Max}_{gL \in G/L} |\ f_\varepsilon'(gL) - f(gL) + f(gL) - f_{\varepsilon'}'(gL)\ |_p \\ &\leq \operatorname{Max}\{\varepsilon, \varepsilon'\}. \end{aligned}$$

On obtient, à partir de cette inégalité générale, d'une part (avec $f_{\varepsilon'}' = f_\varepsilon$) l'inégalité $|\ \langle f_\varepsilon', \mu \rangle - \langle f_\varepsilon, \mu \rangle\ |_p \leq \varepsilon$, et d'autre part $|\ \langle f_{\varepsilon'}, \mu \rangle - \langle f_\varepsilon, \mu \rangle\ | \leq Max\{\varepsilon, \varepsilon'\}$; par conséquent, on a une suite de Cauchy $(\langle f_\varepsilon, \mu \rangle)_\varepsilon$ qui converge vers un nombre de $\mathbb{C}_p$, indépendant du choix de la famille $(f_\varepsilon)_\varepsilon$, noté $\int_G f\ d\mu$, ou plus simplement

$$\langle f, \mu \rangle_G = \langle f, \mu \rangle,$$

et appelé l'intégrale de f sur G par rapport à la mesure μ.

(5.2) **Remarques.** (i) On peut intégrer sur toute partie de G de la forme $U \in \mathcal{U}_G$: il suffit d'intégrer $f\kappa_U$ où κ_U est la fonction caractéristique de U (qui est continue puisque U et $G - U$ sont ouverts) ; on obtient alors $\langle f, \mu\rangle_U$ qui peut s'approcher, à ε près, de la façon suivante : on considère $H \in \Omega_G$ assez petit tel que :

(α) $U = \cup_{i=1}^{n} g_i H$ (union finie disjointe),

(β) pour tout $i = 1, \ldots, n$, $\sup\limits_{x,y \in g_i H} (| f(x) - f(y) |_p) < \varepsilon$;

on a alors, en choisissant des $x_i \in g_i H$, l'approximation à ε près

$$\sum_{i=1}^{n} f(x_i)\, \mu(g_i H).$$

(ii) On vérifie facilement les propriétés de linéarité de l'intégrale.

(5.3) **Cas des caractères continus.** Désignons par X_G le groupe des caractères continus de G à valeurs dans $\mathbb{C}_p$ (X_G contient les caractères d'ordre fini). Pour calculer une intégrale de la forme $\langle \chi, \mu\rangle$, $\chi \in X_G$, on peut utiliser le fait que $\mathbb{Z}_p[G]$ est dense dans Λ_G (cf. (3.2)) : si $\alpha \in \mathbb{Z}_p[G]$, $\alpha = \sum_g a_g\, g$ avec $Supp(\alpha)$ fini, on a $\langle \chi, \alpha\rangle = \sum_g a_g\, \langle \chi, g\rangle$; or, par définition de la mesure de Dirac g, on a $\langle \chi, g\rangle = \chi(g)$ (revenir aux définitions pour s'en convaincre).

D'après ce qui a été fait dans la démonstration de (3.2), si $\mu \in \Lambda_G$ et si $H \in \Omega_G$, tout relèvement de $\mu_H = \sum\limits_{gH \in G/H} \mu(gH) gH$ dans $\mathbb{Z}_p[G]$, donc de la forme $\sum\limits_{gH \in G/H} \mu(gH)\, g$, conduit à l'approximation

$$\langle \chi, \mu_H\rangle = \sum_{gH \in G/H} \mu(gH)\, \chi(g).$$

Nous nous référerons souvent à ce fait très utile en pratique et que nous résumons dans l'énoncé suivant :

(5.3.1) **Théorème.** Soit χ un caractère continu de G dans $\mathbb{C}_p$ et soit $\mu \in \Lambda_G$, $\mu = (\mu_H)_{H \in \Omega_G}$; alors on a

$$\begin{aligned} \langle \chi, \mu\rangle &= \lim_H \langle \chi, \mu'_H\rangle \\ &= \lim_H \langle \chi, \sum_{\sigma \in G/H} \mu(\sigma)\, \sigma'\rangle \\ &= \lim_H \sum_{\sigma \in G/H} \mu(\sigma)\, \chi(\sigma') \end{aligned}$$

où, pour tout $\sigma \in G/H$, σ' désigne un relèvement arbitraire de σ dans G.

(5.3.2) **Remarque.** Si χ est d'ordre fini et si $H = Ker\ \chi$, on a $H \in \Omega_G$ et il vient facilement $\langle \chi, \mu\rangle = \langle \chi, \mu_H\rangle$ (somme finie).

(5.4) **Proposition.** Si λ, $\mu \in \Lambda_G$ et si $\chi \in X_G$, on a

$$\langle \chi, \lambda\mu \rangle = \langle \chi, \lambda \rangle \langle \chi, \mu \rangle.$$

En effet si α, $\beta \in \mathbb{Z}_p[G]$, d'après (I.2.2.2) on a :
$\langle \chi, \alpha\beta \rangle = \chi(\alpha)\,\chi(\beta) = \langle \chi, \alpha \rangle \langle \chi, \beta \rangle$; d'où le résultat par densité.

(5.5) **Remarque.** Cette propriété fait que dans le cas des caractères continus, on pose $\langle \chi, \mu \rangle = \chi(\mu)$, le caractère χ se prolongeant par linéarité et continuité en un homomorphisme de $\mathbb{Z}_p$-algèbres de Λ_G dans $\mathbb{C}_p$ noté encore χ.

(5.6) **Proposition.** Soit G un groupe profini commutatif pour lequel le p-Sylow $G(p)$ est fini, et soit α_G la mesure de Haar sur G (cf. (4.3)). Soit $\chi \in X_G$ (cf. (5.3)) ; alors on a les relations suivantes :
(i) $\langle \chi, \alpha_G \rangle = 0$ si $\chi \neq \chi_0$ (caractère unité de G),
(ii) $\langle \chi, \alpha_G \rangle = \mid G(p) \mid$ si $\chi = \chi_0$.

Si $\chi \neq \chi_0$, il existe $g \in G$ tel que $\chi(g) \neq 1$; écrivons alors que $(1-g)\alpha_G = 0$ et intégrons cette relation en tenant compte de (5.4) ; il vient :

$$(1 - \chi(g))\,\langle \chi, \alpha_G \rangle = 0, \text{ d'où } \langle \chi, \alpha_G \rangle = 0.$$

Si $\chi = \chi_0$, on a d'après (5.3.2) :

$$\langle \chi_0, \alpha_G \rangle = \langle \chi_0, (\alpha_G)_G \rangle = \langle \chi_0, \mid G(p) \mid \rangle = \mid G(p) \mid .$$

6.— $\mathbb{Z}_p$-distributions.

Soit toujours G un groupe profini commutatif, et soit Λ_G la $\mathbb{Z}_p$-algèbre des $\mathbb{Z}_p$-mesures sur G. Une façon d'élargir la notion de mesure est la suivante :

(6.1) **Définitions.** (i) On appelle algèbre des $\mathbb{Z}_p$-distributions sur G l'anneau total des fractions de Λ_G ; c'est donc l'ensemble des fractions $\frac{\nu}{\delta}$, ν, $\delta \in \Lambda_G$, δ non nul et non diviseur de 0 dans Λ_G ;
(ii) On désigne par Δ_G la $\mathbb{Z}_p$-algèbre des distributions sur G ; elle contient Λ_G comme sous-algèbre.

Un type particulier de distributions a été introduit par Serre dans [S1] pour interpréter les fonctions L p-adiques comme intégrales :

(6.2) **Définitions.** (i) On appelle $\mathbb{Z}_p$-pseudo-mesure sur G tout élément μ de Δ_G tel que

$$(1-g)\mu \in \Lambda_G, \text{ pour tout } g \in G.$$

(ii) On désigne par $\widetilde{\Lambda}_G$ le sous-$\mathbb{Z}_p$-module de Δ_G des $\mathbb{Z}_p$-pseudo-mesures ; il contient Λ_G comme sous-module ($\widetilde{\Lambda}_G$ n'est pas une sous-algèbre de Δ_G).

Nous verrons au chapitre suivant comment caractériser $\widetilde{\Lambda}_G$, au moins dans des cas particuliers.

Nous allons maintenant essayer de montrer en quoi les distributions sont rattachées à des "mesures non bornées", telles qu'évoquées dans l'Introduction.

(6.3) **Proposition.** Si G est fini, alors la $\mathbb{Z}_p$-algèbre Δ_G s'identifie canoniquement à $\mathbb{Q}_p[G]$.

(i) Si $\rho = \sum_{g\in G} a_g\, g$, $a_g \in \mathbb{Q}_p$, il existe $d \in \mathbb{Z}_p$, $d \neq 0$, tel que $d\, a_g \in \mathbb{Z}_p$ pour tout $g \in G$; d'où $d\rho \in \mathbb{Z}_p[G]$, et ρ est une distribution de dénominateur d.

(ii) Soit $\rho = \frac{\nu}{\delta} \in \Delta_G$, ν, $\delta \in \mathbb{Z}_p[G]$, $\delta \neq 0$ et non diviseur de 0 dans $\mathbb{Z}_p[G]$; en utilisant la transformée de Fourier de δ (cf. (I.2.3.5)), on sait que ces conditions sur δ ont lieu si et seulement si $\langle \chi, \delta\rangle \neq 0$ pour tout $\chi \in X_G$; on peut donc considérer, pour tout $\chi \in X_G$:

$$\rho_\chi = \frac{\langle \chi, \nu\rangle}{\langle \chi, \delta\rangle}.$$

Soit $\mathbb{Q}_p(\chi)$ (resp. $\mathbb{Z}_p(\chi)$) le corps des valeurs de χ sur $\mathbb{Q}_p$ (resp. son anneau d'entiers) ; comme $\langle \chi, \nu\rangle$, $\langle \chi, \delta\rangle \in \mathbb{Z}_p(\chi)$, il existe $d_\chi \in \mathbb{Z}_p$, multiple de $\langle \chi, \delta\rangle$, et $\alpha_\chi \in \mathbb{Z}_p(\chi)$, tels que $\rho_\chi = \frac{\alpha_\chi}{d_\chi}$. Soit maintenant $d \in \mathbb{Z}_p$ un p.p.c.m. des d_χ et écrivons

$$\rho_\chi = \frac{\beta_\chi}{d} \text{ pour tout } \chi \in X_G,\ \beta_\chi \in \mathbb{Z}_p(\chi)\ ; \tag{6.3.1}$$

soit alors $\nu' = \sum_{\chi\in X_G} \beta_\chi\, e_\chi \in \mathbb{C}_p[G]$, (cf. (I.2.3.2)), et vérifions que, dans Δ_G, on a :

$$\frac{\nu}{\delta} = \frac{\nu'}{d}. \tag{6.3.2}$$

Ceci équivaut à montrer d'abord que $\nu d - \nu'\delta = 0$ dans $\mathbb{C}_p[G]$ et ensuite que $\nu' \in \mathbb{Q}_p[G]$; or, pour tout $\psi \in X_G$ on obtient

$$\psi(\nu)d - \psi(\nu')\psi(\delta) = \rho_\psi\ \psi(\delta)d - \beta_\psi\ \psi(\delta) = 0 \text{ d'après (6.3.1).}$$

Montrons enfin que $\nu' \in \mathbb{Q}_p[G]$; par construction, on a $\nu' \in \mathbb{Q}_p(\xi)[G]$, où ξ est une racine de l'unité d'ordre diviseur de $|\ G\ |$. Tout $\mathbb{Q}_p$-automorphisme s de $\mathbb{Q}_p(\xi)$ s'étend de façon canonique en un $\mathbb{Q}_p[G]$-automorphisme (noté s) de $\mathbb{Q}_p(\xi)[G]$ et la théorie de Galois s'y applique (coefficient par coefficient) ; or la relation (6.3.2) conduit à

$$s(\nu)d = s(\delta)s(\nu'),$$

soit $\nu d = \delta s(\nu')$, puisque ν, d, $\delta \in \mathbb{Z}_p[G]$, auquel cas $\nu' \in \mathbb{Q}_p[G]$ et $\rho = \frac{\nu}{\delta} = \frac{\nu'}{d} \in \mathbb{Q}_p[G]$.

(6.3.3) **Remarques.** (i) On peut se demander ce qu'il advient de (6.3) dans le cas où G est infini. Le problème est que si $\rho = \frac{\nu}{\delta} \in \Delta_G$, il se peut que dans les $\mathbb{Z}_p[G/H]$, $H \in \Lambda_G$, certains δ_H soient nuls ou diviseurs de 0, alors que dans le cas G fini, si δ est non nul et non diviseur de 0 dans $\mathbb{Z}_p[G]$, δ_H est non nul et non diviseur de 0 dans $\mathbb{Z}_p[G/H]$ (il suffit

d'utiliser la transformée de Fourier en remarquant que $\Phi_{G/H}(f) = (\chi(f))_\chi$, $\chi \in X_{G/H}$ (où $X_{G/H}$ est identifié à $\{\chi \in X_G, Ker\chi \supseteq H\}$).

Par contre dans le cas G infini, si pour tout $H \in \Lambda_G$, δ_H est non nul et non diviseur de 0 dans $\mathbb{Z}_p[G/H]$ (condition équivalente à $\chi(\delta) \neq 0$ pour tout caractère χ d'ordre fini de G), alors $\rho_H = \frac{\nu_H}{\delta_H}$ a un sens dans $\Delta_{G/H} = \mathbb{Q}_p[G/H]$ (d'après (6.3)), et par conséquent on a

$$(\rho_H)_H \in \varprojlim_{H \in \Omega_G} \mathbb{Q}_p[G/H].$$

On notera que ρ_H est bien indépendant de l'écriture fractionnaire $\rho = \frac{\nu}{\delta}$, à condition de se restreindre aux dénominateurs δ dont les projections δ_H sont nulles et non diviseurs de 0.

(ii) La réciproque est inexacte : on peut avoir une famille cohérente $(\rho_H)_H \in \varprojlim_H \mathbb{Q}_p[G/H]$, sans qu'il existe $\frac{\nu}{\delta} \in \Delta_G$ (δ_H non nul et non diviseur de 0 pour tout $H \in \Omega_G$) telle que $\rho_H = \frac{\nu_H}{\delta_H}$ dans $\mathbb{Q}_p[G/H]$: par exemple, considérons $G \simeq \mathbb{Z}_p$, où $\Omega_G = \{H_n = G^{p^n}, n \geq 0\}$ et posons

$$\rho_{H_n} = \rho_n = p^{-n} \sum_{\tau_n \in G/H_n} \tau_n \ ;$$

on a $(\rho_n)_n \in \varprojlim_n \mathbb{Q}_p[G/H_n]$ de façon évidente, et s'il existait ν, $\delta \in \Lambda_G$ telles que $\rho_n \delta_n = \nu_n$ pour tout n, on aurait en particulier

$$\nu_n = p^{-n}\Big(\sum_{\tau_n} \tau_n\Big)\delta_n = p^{-n}\Big(\sum_{\tau_n} \tau_n\Big)\langle \chi_0, \delta_n\rangle$$

(puisque $\tau \sum_{\tau_n} \tau_n = \sum_{\tau_n} \tau_n$ pour tout $\tau \in G/H_n$), soit $\nu_n = p^{-n}\delta_0 \sum_{\tau_n} \tau_n$ où $\delta_0 \in \mathbb{Z}_p$; puisque $\nu_n \in \mathbb{Z}_p[G/H_n]$, on a nécessairement $\delta_0 \equiv 0 \bmod p^n$ pour tout n, soit $\delta_0 = 0$ et $\nu_n = 0$, ce qui est absurde (cf. (4.5) au sujet des mesures invariantes par translation dans le cas $G(p)$ non fini).

En conclusion, par rapport à la notion de $\mathbb{Z}_p$-mesure, il y a 2 niveaux de généralisation qui se dégagent :

(i) les $\mathbb{Z}_p$-distributions $\rho = \frac{\nu}{\delta}$ pour lesquelles δ_H est non nul et non diviseur de 0 dans $\mathbb{Z}_p[G/H]$, pour tout $H \in \Omega_G$;

(ii) les autres $\mathbb{Z}_p$-distributions pour lesquelles tout caractère d'ordre fini n'est pas nécessairement intégrable.

(6.3.4) **Notation**. On désigne par Δ'_G la sous-algèbre de Δ_G formée des $\mathbb{Z}_p$-distributions $\rho = \frac{\nu}{\delta}$ pour lesquelles δ_H est non nul et non diviseur de 0 dans $\mathbb{Z}_p[G/H]$, pour tout $H \in \Omega_G$.

Les éléments de Δ'_G sont donc des éléments particuliers de $\varprojlim \mathbb{Q}_p[G/H]$; ce sera le cas des "distributions de Stickelberger" qui seront étudiées au chapitre IV ; par contre, les pseudo-mesures non triviales sont dans $\Delta_G - \Delta'_G$.

(6.3.5) **Définition**. Soit $tor(X_G)$ le sous-groupe de X_G formé des caractères d'ordre fini de G ; on appelle transformée de Fourier l'application Φ de $\Theta_G = \varprojlim_{H \in \Omega_G} \mathbb{C}_p[G/H]$ dans

$\prod_{\chi \in tor(X_G)} \mathbb{C}_p$ qui à $\xi = (\xi_H)_H$ associe la famille $(\chi(\xi))_\chi$, où $\chi(\xi) = \chi(\xi_H)$ pour n'importe quel $H \in \Omega_G$ contenu dans $Ker\ \chi$.

Ceci définit un homomorphisme injectif de $\mathbb{C}_p$-algèbres, qui coïncide avec l'application définie en (I.2.3) lorsque G est fini. Comme Δ_G' est une sous- $\mathbb{Z}_p$-algèbre de Θ_G, la transformée de Fourier de $\rho = \frac{\nu}{\delta}$, ν, $\delta \in \Lambda_G$, δ_H non nul et non diviseur de 0 dans $\mathbb{Z}_p[G/H]$ pour tout $H \in \Omega_G$, est donné par

$$\Phi(\rho) = \left(\chi(\nu)\chi(\delta)^{-1}\right)_{\chi \in tor(X_G)} .$$

(6.4) **Intégration par rapport à une distribution.** Si $\rho = \frac{\nu}{\delta} \in \Delta_G$, on ne peut définir, a priori, l'intégrale d'une fonction quelconque, mais uniquement l'intégrale d'un caractère continu, ou plus généralement d'une combinaison $\mathbb{C}_p$-linéaire finie de tels caractères.

(6.4.1) **Définition.** Soit $\rho = \frac{\nu}{\delta} \in \Delta_G$, ν, $\delta \in \Lambda_G$, δ non nul et non diviseur de 0, et soit $f = \sum_{i=1}^n c_i\chi_i$, $c_i \in \mathbb{C}_p$, $\chi_i \in X_G$ distincts. Alors si $\langle \chi_i, \delta \rangle \neq 0$ pour tout i, on définit $\int_G f d\rho$ par

$$\begin{aligned} \langle f, \rho \rangle &= \sum_{i=1}^n c_i \langle \chi_i, \nu \rangle \langle \chi_i, \delta \rangle^{-1} \\ &= \sum_{i=1}^n c_i \chi_i(\nu)\chi_i(\delta)^{-1}. \end{aligned}$$

On notera que la définition a un sens car d'une part les intégrales $\chi_i(\rho)$ sont définies en raison de la propriété (5.4) des caractères, et, d'autre part, l'écriture de f comme combinaison $\mathbb{C}_p$-linéaire de caractères est unique en raison de l'indépendance linéaire des caractères.

Le résultat suivant montre une possibilité de définition générale :

(6.4.2) **Lemme.** Si f est une fonction de G à valeurs dans $\mathbb{C}_p$, localement constante modulo $H \in \Omega_G$, alors f s'écrit de façon unique comme combinaison $\mathbb{C}_p$-linéaire de caractères d'ordres finis de G.

Appelons f_H l'application de G/H dans $\mathbb{C}_p$ issue de f et définie par $f_H(gH) = f(x)$ pour n'importe quel $x \in gH$; alors le résultat pour f_H est donné par la propriété (I.2.3.4) ; l'écriture de f s'en déduisant trivialement.

CHAPITRE III

Théorèmes de décomposition de Λ_G et $\widetilde{\Lambda}_G$

On fixe une fois pour toutes un nombre premier p. Le but de ce chapitre est de préciser la structure de Λ_G et $\widetilde{\Lambda}_G$ lorsque le p-Sylow de G est, modulo la p-torsion, un $\mathbb{Z}_p$-module de type fini.

1.— Structure de $\mathbb{Z}_p$-module des pro-p-groupes commutatifs.

Comme expliqué en (I, §5) un groupe profini G est dit, par extension du cas fini, un pro-p-groupe, si G coïncide avec son p-Sylow ou encore si G est limite projective de p-groupes finis G_i ; en particulier on a que G/H est un p-groupe fini pour tout $H \in \Omega_G$.

Soit G un pro-p-groupe commutatif et soit $\gamma \in G$; la suite γ^{p^n} converge vers 1 dans G : en effet, si l'on considère un élément du système fondamental standard de voisinages de 1 dans G, de la forme $V_J = \prod_{i \in I-J} G_i \times \prod_{j \in J} \{1_j\}$, $J \subset I$, J fini, on a $\gamma^{p^n} \in V_J$ dès que p^n est multiple de l'exposant des G_j pour tout $j \in J$. Ceci veut dire que l'application suivante (pour $\gamma \in G$ fixé) :

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ x & & \gamma^x \end{array}$$

est continue lorsque $\mathbb{Z}$ est muni de la topologie p-adique ; elle se prolonge donc en une application continue f_γ de $\mathbb{Z}_p$ dans G qui est un homomorphisme de groupes topologiques. On a ainsi sur G une structure canonique de $\mathbb{Z}_p$-module que nous utiliserons constamment.

L'application f_γ est injective si et seulement si $o(\gamma) = p^\infty$.
L'image de $\mathbb{Z}_p$ par f_γ, qui est donc le $\mathbb{Z}_p$-module engendré par γ, s'appelle le sous-groupe de G engendré topologiquement par γ, sous-groupe pour lequel on dit que γ est un générateur topologique (ou, par abus, un générateur) et que l'on note $\gamma^{\mathbb{Z}_p}$.

En résumé, si $\gamma \in G$, on a

$$\gamma^{\mathbb{Z}_p} \simeq \mathbb{Z}/p^n\mathbb{Z} \text{ ou } \mathbb{Z}_p$$

selon que $o(\gamma) = p^n$ ou p^∞.

(1.1) **Remarque**. Il est clair que $\gamma^{\mathbb{Z}_p}$ est l'adhérence dans G du groupe $\gamma^{\mathbb{Z}}$ engendré (algébriquement) par γ. Comme seuls les sous-groupes fermés ont un intérêt ici, on utilisera toujours l'engendrement pour la structure de $\mathbb{Z}_p$-module.

(1.2) **Conséquences**. Soit G un pro-p-groupe commutatif ; on désigne par $tor(G)$ le sous-$\mathbb{Z}_p$-module de torsion de G, qui est donc égal à $\{g \in G,\ o(g) = p^n,\ n \in \mathbb{N}\}$. On a alors les faits suivants :

(i) Si G admet un quotient G/A, A fermé (*), qui est un $\mathbb{Z}_p$-module de type fini sans torsion, alors il existe un sous-module libre de dimension finie Γ de G tel que

$$G = A \oplus \Gamma.$$

(*) cette condition est nécessaire pour que le quotient soit un pro-p-groupe et par là un $\mathbb{Z}_p$-module.

En effet, si G/A est de type fini comme $\mathbb{Z}_p$-module et sans torsion, il est libre ($\mathbb{Z}_p$ est principal), et on peut écrire

$$G/A = \bigoplus_{i=1}^{r} (\gamma_i A)^{\mathbb{Z}_p},\ \gamma_i \in G,\ (\gamma_i A)^{\mathbb{Z}_p} \simeq \mathbb{Z}_p,$$

auquel cas on vérifie facilement que

$$G = A \oplus \Gamma,\ \text{où}\ \Gamma = \bigoplus_{i=1}^{r} \gamma_i^{\mathbb{Z}_p}.$$

(ii) En particulier si $G/tor(G)$ est de type fini, alors il existe un sous-module Γ de G, $\Gamma \simeq \mathbb{Z}_p^r$, tel que $G = tor(G) \oplus \Gamma$ (le nombre r est alors le $\mathbb{Z}_p$-rang de G).

(iii) Enfin si G est lui-même un $\mathbb{Z}_p$-module de type fini, on a en outre $tor(G) \simeq \prod_{i=1}^{s} \mathbb{Z}/p^{n_i}\mathbb{Z}$, $s \geq 0$, $1 \leq n_1 \leq \ldots \leq n_s$.

2.— Décomposition d'un groupe profini commutatif.

Comme dans le cas fini, on a le fait suivant, pour G profini commutatif quelconque :

(2.1) **Lemme.** On a $G = G_0 \oplus G(p)$, où G_0 (resp. $G(p)$) est le sous-groupe des éléments de G d'ordre étranger à p (resp. d'ordre puissance de p) (cf. (I, §5)).

Les vérifications du fait que G_0 et $G(p)$ sont des sous-groupes ($G(p)$ étant le p-Sylow de G) sont élémentaires, comme la vérification du fait que $G_0 \cap G(p) = \{1\}$. Si $x \in G$, dans l'écriture $G = \varprojlim_{i \in I} G_i$, on peut décomposer x sous la forme $x = (x_{i,0} \times x_{i,p})_i$, où $x_{i,0}$ (resp. $x_{i,p}$) est d'ordre étranger à p (resp. d'ordre puissance de p) ; on vérifie que $x_0 = (x_{i,0})_i$ et $x_p = (x_{i,p})_i$ sont dans $\varprojlim_{i \in I} G_i$ (les h_{ij} respectant la nature des ordres des éléments), auquel cas $x = x_0 x_p$, $x_0 \in G_0$, $x_p \in G(p)$.

(2.2) **Corollaire.** On a $G = \prod_p G(p)$ (p premiers).

(2.3) **Remarque.** On peut retrouver ces résultats directement en écrivant $G_i = \oplus_p G_i(p)$ et en vérifiant que, d'une manière générale, on a

$$\varprojlim_{i \in I} \bigoplus_p G_i(p) \simeq \prod_p \varprojlim_{i \in I} G_i(p).$$

Selon ce point de vue, on obtient immédiatement que $\widehat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p$ (cf. (I.3.6.1)).

Nous ferons désormais l'hypothèse suivante qui se trouve être vérifiée pour toutes les applications à l'arithmétique (en particulier par le fait que les groupes de Galois issus de la théorie du corps de classes au-dessus d'un corps de nombres vérifient cette hypothèse) :

(2.4) **Hypothèse** (H_p). On supppose que le groupe profini commutatif G possède, pour le nombre premier p considéré, un p-sous-groupe de Sylow $G(p)$ pour lequel $G(p)/tor(G(p))$ est de type fini comme $\mathbb{Z}_p$-module (donc $\mathbb{Z}_p$-libre de rang $r \geq 0$ fini).

Il résulte de cette hypothèse que

$$G(p) = tor(G(p)) \oplus \bigoplus_{i=1}^{r} \Gamma_i,\ \Gamma_i \simeq \mathbb{Z}_p \text{ pour } 1 \leq i \leq r;$$

de même, G peut alors s'écrire (cf. (2.1)) :

$$G = G_0 \oplus tor(G(p)) \oplus \bigoplus_{i=1}^{r} \Gamma_i$$

(sans qu'il soit nécessaire de supposer $tor(G(p))$ de type fini) ; enfin, si l'on veut privilégier une composante isomorphe à $\mathbb{Z}_p$, lorsque $r \geq 1$, on peut écrire (de façon non unique) :

(2.4.1) $$G = A \oplus \Gamma,\ \Gamma \simeq \mathbb{Z}_p.$$

(2.4.2) **Remarque.** C'est le point de départ de l'étude de $\widetilde{\Lambda}_G$ (cf. (II.6.2)) dans [S1] ; on notera que le p-Sylow de A peut être infini pour 2 raisons : soit que l'on a $r \geq 2$, soit que $tor(A(p))$ n'est pas de type fini, cas qui se produit si G est groupe de Galois de l'extension abélienne maximale d'un corps de nombres k, mais qui n'a plus lieu si l'on se restreint au groupe de Galois de l'extension abélienne S-ramifiée maximale de k, lorsque S est un ensemble fini de places de k (cf. chap. IV, §1).

(2.5) **Caractères continus de G.** Restreignons-nous au p-Sylow $G(p)$ de G, en supposant que $G(p)$ est un $\mathbb{Z}_p$-module de type fini. Ecrivons $G(p) = tor(G(p)) \oplus \bigoplus_{i=1}^{r} \Gamma_i$, $\Gamma_i \simeq \mathbb{Z}_p$, où l'on suppose donc $tor(G(p))$ fini.

Soit $X_{G(p)}$ le groupe des caractères continus de $G(p)$ dans $\mathbb{C}_p^\times$. Comme dans le cas classique, on vérifie que

$$X_{G(p)} \simeq X_{tor(G(p))} \oplus \bigoplus_{i=1}^{r} X_{\Gamma_i} \text{ (non canoniquement).}$$

On est ramené à étudier :
X_B pour un p-groupe fini B, ce qui est clair,
X_Γ pour $\Gamma \simeq \mathbb{Z}_p$.

(2.5.1) **Lemme.** Le groupe X_Γ est isomorphe au sous-groupe $\mathcal{U}_p$ de $\mathbb{C}_p^\times$ formé des unités principales (i.e. des $u \in \mathbb{C}_p^\times$ tels que $| u - 1 |_p < 1$).

Soit γ un générateur topologique de Γ, soit χ un élément de X_Γ et posons

$$u = \chi(\gamma);$$

comme $u^{p^n} = \chi(\gamma^{p^n})$, par continuité, $u^{p^n} \to 1$ si $n \to \infty$; par conséquent, $| u |_p^{p^n} \to 1$, et $| u |_p = 1$ nécessairement. De plus on a $| u - 1 |_p < 1$ car sinon, si $u = 1 + v$ avec $| v |_p \geq 1$, on peut écrire $u^{p^n} - 1 = \prod(u - \zeta)$, où ζ parcourt le groupe μ_{p^n} des racines p^n-ièmes de l'unité ; or $u - \zeta = u - 1 + 1 - \zeta = v + 1 - \zeta$, et $| u - \zeta |_p = | v + 1 - \zeta |_p = | v |_p$ puisque $| 1 - \zeta |_p < 1$ et $| v |_p \geq 1$; on aurait donc $| u^{p^n} - 1 |_p = | v |_p^{p^n} \geq 1$, ce qui est absurde.

Ecrivons alors $u = 1 + \pi \in \mathcal{U}_p$ avec $| \pi |_p < 1$; on vérifie, par récurrence sur n, que $(1 + \pi)^{p^n} = 1 + \pi_n$ avec $| \pi_n |_p \to 0$.
D'où le lemme facilement.

(2.5.2) **Remarque.** Les éléments de μ_{p^n}, $n \in \mathbb{N}$, sont dans $\mathcal{U}_p$, et on retrouve ainsi les caractères d'ordre fini de Γ.

3.— Algèbres de séries formelles.

Nous allons montrer, toujours dans le cadre de l'hypothèse (H_p) faite en (2.4), que l'on peut interpréter l'algèbre Λ_G comme une algèbre de séries formelles. Le résultat est le suivant (où p est un nombre premier fixé) :

(3.1) **Théorème.** Soit G un groupe profini commutatif vérifiant l'hypothèse (H_p) ; on fixe une décomposition de la forme $G = A \oplus \Gamma$, $\Gamma \simeq \mathbb{Z}_p$ (cf. (2.4.1)) et un générateur topologique γ de Γ. Soit $\Lambda_A[[T]]$ munie de la topologie de la convergence simple des coefficients. Alors il existe un unique homéomorphisme de Λ_A-algèbres topologiques qui transforme T en $1-\gamma$.

démonstration

Pour décrire $\Lambda_G = \varprojlim \mathbb{Z}_p[G/H]$, $H \in \Omega_G$, on peut remplacer Ω_G par la partie cofinale suivante (cf. (I.3.5)) :

$$\Omega_G' = \{B \oplus \Gamma_n,\ B \in \Omega_A,\ \Gamma_n = \Gamma^{p^n},\ n \geq 0\},$$

sur laquelle l'ordre est l'ordre produit (i.e. $B' \oplus \Gamma_m \geq B \oplus \Gamma_n$ si et seulement si on a $B' \subseteq B$ et $\Gamma_m \subseteq \Gamma_n$, soit $m \geq n$). Il vient alors :

$$\begin{aligned}\Lambda_G &= \varprojlim \mathbb{Z}_p[A \oplus \Gamma / B \oplus \Gamma_n] \\ &\simeq \varprojlim_{B,n} \mathbb{Z}_p[A/B \times \Gamma/\Gamma_n] \\ &\simeq \varprojlim_{B,n} \mathbb{Z}_p[A/B]\,[\Gamma/\Gamma_n]\end{aligned}$$

(en utilisant des isomorphismes de systèmes projectifs évidents).

(3.1.1) **Lemme.** On a $\varprojlim_{B,n} \mathbb{Z}_p[A/B]\,[\Gamma/\Gamma_n] \simeq \varprojlim_{n} \Lambda_A[\Gamma/\Gamma_n]$.

La première limite projective est un sous-anneau de $\prod_{B,n} \mathbb{Z}_p[A/B]\,[\Gamma/\Gamma_n]$, $B \in \Omega_A$, $n \geq 0$, produit qui peut s'écrire $\prod_n \left(\prod_B \mathbb{Z}_p[A/B]\,[\Gamma/\Gamma_n]\right)$.

Considérons un élément α de $\varprojlim_{B,n} \mathbb{Z}_p[A/B]\,[\Gamma/\Gamma_n]$; il s'écrit

$$\alpha = (\alpha_{B,n})_{B,n},\ \alpha_{B,n} = \sum_{i \bmod p^n} a^i_{B,n} \gamma^i_n, \tag{3.1.2}$$

où $a^i_{B,n} \in \mathbb{Z}_p[A/B]$, $\gamma_n = \gamma\Gamma_n$ dans Γ/Γ_n.

A α associons les familles suivantes ($n \geq 0$, $1 \leq i \leq p^n$) :

$$a^i_n = (a^i_{B,n})_B,\ B \in \Omega_A\ ; \tag{3.1.3}$$

pour n et i fixés, la famille obtenue dans $\prod_B \mathbb{Z}_p[A/B]$ est cohérente (à n fixé), les $\alpha_{B,n}$ sont cohérents en B et la cohérence passe aux coefficients sur la base des γ_n^i, $1 \leq i \leq p^n$ (cf. (3.1.2)) ; à α on a donc associé l'élément

$$\alpha_n = \sum_{i \bmod p^n} a_n^i \gamma_n^i \in \Lambda_A[\Gamma/\Gamma_n] \,. \tag{3.1.4}$$

Dans (3.1.2), la cohérence de α, cette fois à B fixé, s'exprime pour tout m, $n \in \mathbb{N}$, $m \geq n$, par les relations suivantes (dans la projection $\Gamma_m \to \Gamma_n$) :

$$\sum_{j \bmod p^m} a_{B,m}^j \gamma_n^j = \sum_{i \bmod p^n} a_{B,n}^i \gamma_n^i,$$

soit :

$$a_{B,n}^i = \sum_{\lambda=0}^{p^{m-n}-1} a_{B,m}^{\lambda p^n + i}, \; i \bmod p^n, \tag{3.1.5}$$

ce qui (à m et n fixés) permet d'écrire, dans la limite projective sur B, compte-tenu de (3.1.3) :

$$a_n^i = \sum_{\lambda=0}^{p^{m-n}-1} a_m^{\lambda p^n + i}, \; i \bmod p^n,$$

qui traduit la cohérence dans $\varprojlim_n \Lambda_A[\Gamma/\Gamma_n]$, de la famille

$$\alpha' = \left(\sum_{i \bmod p^n} a_n^i \gamma_n^i \right)_n = (\alpha_n)_n \quad \text{(cf. (3.1.4))}.$$

On vérifie point par point que l'application qui à α (cf. (3.1.2)) associe α' est l'isomorphisme cherché.

Il reste alors à interpréter

$$\varprojlim_n \Lambda_A[\Gamma/\Gamma_n].$$

On a alors le résultat suivant qui généralise une démonstration classique ayant son origine dans la théorie d'Iwasawa (cf. [L], [S3]) :

(3.1.6) **Lemme**. Soit R une $\mathbb{Z}_p$-algèbre topologique unitaire compacte. Alors il existe un unique isomorphisme de R-algèbres topologiques de $\varprojlim_n R[\Gamma/\Gamma_n]$ sur $\Lambda = R[[T]]$ qui à γ associe $1 - T$ (on rappelle que $R[\Gamma]$ peut être identifiée à une sous-algèbre de $\varprojlim_n R[\Gamma/\Gamma_n]$, comme on l'a fait en (II.3.1.2) dans le cas de $R = \mathbb{Z}_p$).

Soit P_n le polynome $(1-T)^{p^n}-1 \in \mathbb{Z}_p[T]$, $n \geq 0$; on a les diagrammes commutatifs suivants (pour $m \geq n$) :

$$\begin{array}{ccc} R[\Gamma/\Gamma_m] & \xrightarrow{f_m} & R[T]/(P_m) \\ h_{m,n} \downarrow & & \downarrow h'_{m,n} \\ R[\Gamma/\Gamma_n] & \xrightarrow{f_n} & R[T]/(P_n) \end{array}$$

Le R-isomorphisme f_n résulte du fait que Γ/Γ_n est cyclique d'ordre p^n et engendré par $\gamma_n = \gamma\Gamma_n$; on a donc $R[\Gamma/\Gamma_n] \simeq R[X]/(X^{p^n}-1)$ et il suffit de faire le changement d'indéterminée $X \to 1-T$ (on a donc bien associé T et $1-\gamma_n$). Le R-homomorphisme $h'_{m,n}$ existe puisque P_n divise P_m (car $X^{p^n}-1$ divise $X^{p^m}-1$, pour tout $m \geq n$). La commutativité du diagramme vient du fait que

$$\begin{aligned} h'_{m,n} \circ f_m(\gamma_m) &= h'_{m,n}(1-T \bmod P_m) \\ &= 1-T \bmod P_n, \end{aligned}$$

et

$$f_n \circ h_{m,n}(\gamma_n) = f_n(\gamma_n) = 1-T \mod P_n.$$

On a donc un R-isomorphisme de systèmes projectifs (cf. (I.3.4)) qui conduit à

$$\varprojlim_n R[\Gamma/\Gamma_n] \simeq \varprojlim_n R[T]/(P_n),$$

et dans cet isomorphisme, $(\gamma_n)_n = \gamma$ correspond à $1-T$.

(3.1.7) **Lemme**. On a $R[T]/(P_n) \simeq R[[T]]/P_nR[[T]]$.

Soit $S \in \Lambda = R[[T]]$, $S = \sum_{i\geq 0} s_i\, T^i$, $s_i \in R$, et pour tout $m \geq 0$ posons $S_m = \sum_{i=0}^{mp^n-1} s_i\, T^i$. Soit $\mathfrak{A}$ l'idéal (P_n, p^m) de Λ ; comme $P_n = (1-T)^{p^n}-1$, on a $T^{p^n} \in (P_n, p)$, d'où $T^{mp^n} \in \mathfrak{A}$; par division euclidienne de S_m par P_n dans $R[T]$, il vient $S_m = Q_mP_n + R_m$, avec degré $(R_m) < p^n$. D'où $S \equiv R_m \bmod \mathfrak{A}$, et on peut écrire $S = R_m + A_mP_n + B_mp^m$, A_m, $B_m \in \Lambda$.
Comme Λ est compacte, il existe $R \in R[T]$, de degré $< p^n$, et $A \in \Lambda$, tels que $S = R + AP_n$ dans Λ puisque, par hypothèse, $p^m.1 \to 0$ dans R.

Tout revient maintenant à montrer, comme pour le cas des groupes profinis, que $\varprojlim_n \Lambda/P_n\Lambda$ "redonne" Λ.
Pour cela, considérons l'homomorphisme

$$\begin{aligned} \Lambda &\longrightarrow \prod_n \Lambda/P_n\Lambda \\ x &\longrightarrow (x \bmod P_n)_n \end{aligned}$$

dont le noyau est $\cap_n P_n\Lambda$. On remarque que $P_n \in (p,T)^{n+1}$:

en effet, on a pour tout $n \geq 0$:

$$P_{n+1}/P_n = 1 + (1-T)^{p^n} + \cdots + (1-T)^{p^n(p-1)} \in (p,T),$$

d'où le résultat puisque $P_0 = -T \in (p,T)$. Or l'idéal $(p,T)^{n+1}$ est égal au R-module

$$p^{n+1}R + p^nTR + \cdots + pT^nR + T^{n+1}\Lambda.$$

Donc si $x = \sum_{i\geq 0} a_iT^i \in P_n\Lambda$, on a en particulier

$$\sum_{i\geq 0} a_iT^i \equiv p^{n+1}b_0 + p^nTb_1 + \cdots + pT^nb_n \mod T^{n+1}\Lambda,$$

soit

$$\begin{aligned} a_0 &\in p^{n+1}R, \\ a_1 &\in p^nR, \\ &\vdots \\ a_n &\in pR. \end{aligned}$$

Il résulte de ceci que si $x \in \cap_n P_n\Lambda$, alors, pour tout $i \geq 0$ fixé, on a :

$$a_i \in \bigcap_m p^mR,$$

soit $a_i = 0$.
L'application définie est donc injective et prend ses valeurs dans $\varprojlim_n \Lambda/P_n\Lambda$.

Vérifions enfin la surjectivité :
Si $(x_n + P_n\Lambda)_n \in \varprojlim_n \Lambda/P_n\Lambda$, la cohérence implique en particulier que, pour $m \geq n$, on a

$$x_m \equiv x_n \mod P_n\Lambda,$$

soit

$$x_m - x_n \in (p,T)^{n+1}.$$

Or pour la topologie de la convergence simple des coefficients on peut dire, d'après les calculs antérieurs, que $(p,T)^{n+1}$ tend vers 0 avec n, autrement dit, la suite $(x_n)_n$ est une suite de Cauchy qui est donc ici convergente dès que R est supposée complète. On vérifie que la limite $x \in \Lambda$ convient.

Ceci achève la démonstration du théorème.

(3.2) **Remarque.** Si $\chi \in X_G$, on peut écrire χ sous la forme $\chi = \chi_A\chi_\Gamma$, $\chi_A \in X_A$, $\chi_\Gamma \in X_\Gamma$; on a alors, pour $\lambda = \sum_{i\geq 0} a_iT_i \in \Lambda_A[[T]]$,

$$\langle \chi, \lambda \rangle = \sum_{i\geq 0} \langle \chi_A, a_i \rangle (1 - \chi_\Gamma(\gamma))^i;$$

si $\chi_\Gamma(\gamma) = u$, on a $(1-u)^i \to 0$ (cf.(2.5.1)), et la série ci-dessus est bien convergente dans $\mathbb{C}_p$.

(3.3) **Corollaire.** Si $G = A \oplus \bigoplus_{i=1}^r \Gamma_i$, $\Gamma_i \simeq \mathbb{Z}_p$ pour tout i, il existe un Λ_A-isomorphisme topologique unique de Λ_G sur $\Lambda_A[[T_1, \ldots, T_r]]$ qui à un système de progénérateurs fixés $\gamma_1, \ldots, \gamma_r$ de $\Gamma_1, \ldots, \Gamma_r$ associe $1 - T_1, \ldots, 1 - T_r$.

Nous pouvons alors, dans ce cadre algébrique de séries formelles, donner le théorème de structure du $\mathbb{Z}_p$-module $\widetilde{\Lambda}_G$ des $\mathbb{Z}_p$-pseudo-mesures (cf. (II.6.2)) donné par Serre dans [S1] :

(3.4) **Théorème.** Soit G un groupe profini commutatif vérifiant l'hypothèse (H_p) et possédant un quotient isomorphe à $\mathbb{Z}_p$ (cf. (2.4)), soit $G = A \oplus \Gamma$, $\Gamma \simeq \mathbb{Z}_p$, une décomposition de G, et soit Λ_G identifiée à $\Lambda_A[[T]]$.
Alors on a les faits suivants :

(i) Si $A(p)$ est infini, $\widetilde{\Lambda}_G = \Lambda_G = \Lambda_A[[T]]$;

(ii) si $A(p)$ est fini, $\widetilde{\Lambda}_G = \mathbb{Z}_p \alpha_A T^{-1} + \Lambda_A[[T]]$, où α_A est la mesure de Haar sur A (cf. (II.4.3)).

démonstration

Si $\rho \in \widetilde{\Lambda}_G$ est une $\mathbb{Z}_p$-pseudo-mesure, on a en particulier $T\rho \in \Lambda_G$, soit $T\rho = \sum_{i \geq 0} a_i T^i$, $a_i \in \Lambda_A$; de plus, pour tout $a \in A$, on a aussi $(1-a)\rho \in \Lambda_G$, donc

$$T(1-a)\rho = \sum_{i \geq 0} (1-a) a_i T^i \in T\Lambda_G,$$

ce qui, par identification, conduit à :

$$(1-a)a_0 = 0 \text{ pour tout } a \in A;$$

autrement dit, a_0 est une $\mathbb{Z}_p$-mesure invariante par translation dans Λ_A et donc, d'après (II.4.3), soit nulle soit de la forme $c\alpha_A$, $c \in \mathbb{Z}_p$, selon que $A(p)$ est infini ou non.
D'où le théorème.

CHAPITRE IV

Distributions de Stickelberger

Nous allons introduire des groupes profinis qui sont les groupes de Galois d'extensions abéliennes de $\mathbb{Q}$; il s'agit donc du corps de classes sur $\mathbb{Q}$ dont les résultats sont classiques et se ramènent exclusivement aux propriétés élémentaires des corps cyclotomiques. Les distributions (de Stickelberger) qui existent sur ces groupes de Galois éclairent de façon complète un certain nombre de propriétés arithmétiques des corps abéliens sur $\mathbb{Q}$, notamment par l'intermédiaire des fonctions L p-adiques de $\mathbb{Q}$ qui sont des intégrales par rapport à ces distributions.

Comme les groupes utilisés sont des groupes de Galois, nous modifions systématiquement les notations utilisées jusqu'à présent en utilisant la correspondance entre sous-corps et sous-groupes fermés ; dans cette correspondance, une projection $G = Gal(K/\mathbb{Q}) \to G/H$ est remplacée par une restriction de K à $F = K^H$, etc... Ceci est justifié par la nature des objets utilisés.

1.— Corps cyclotomiques sur $\mathbb{Q}$.

(1.1) **Notations.** (i) Si m est un entier strictement positif, on désigne par $\mathbb{Q}(m)$ le corps cyclotomique des racines m-ièmes de l'unité.

On note G_m le groupe $Gal(\mathbb{Q}(m)/\mathbb{Q})$ qui est canoniquement isomorphe à $(\mathbb{Z}/m\mathbb{Z})^*$ via l'homomorphisme :

$$\sigma_{\cdot,\mathbb{Q}(m)} : (\mathbb{Z}/m\mathbb{Z})^* \to G_m$$

qui à $a + m\mathbb{Z}$, $(a,m) = 1$, associe le $\mathbb{Q}$-automorphisme de $\mathbb{Q}(m)$ qui élève toute racine m-ième de l'unité à la puissance a. Par extension des classes modulo m on définit $\sigma_{a,\mathbb{Q}(m)}$, pour $a \in \mathbb{Q}^\times$, $(a,m) = 1$, et ses restrictions aux sous-corps F de $\mathbb{Q}(m)$ sont notées $\sigma_{a,F}$.

L'élément $\sigma_{a,\mathbb{Q}(m)}$ n'est pas tout à fait le symbole d'Artin de a, car la définition "corps de classes" du symbole d'Artin repose, comme l'on sait, sur l'utilisation du groupe des idéaux I_m de $\mathbb{Q}$ formé des idéaux (a), $a \in \mathbb{Q}^\times, (a,m) = 1$, et généralise l'automorphisme de Frobenius

$$\left(\frac{\mathbb{Q}(m)/\mathbb{Q}}{(\ell)}\right),\ \ell \text{ premier},$$

par multiplicativité :

$$\left(\frac{\mathbb{Q}(m)/\mathbb{Q}}{(a)}\right) = \prod_\ell \left(\frac{\mathbb{Q}(m)/\mathbb{Q}}{(\ell)}\right)^{n_\ell}$$

si $a = \pm\prod \ell^{n_\ell} \in \mathbb{Q}^\times$ est étranger à m ; or $\left(\frac{\mathbb{Q}(m)/\mathbb{Q}}{(\ell)}\right)$ est l'automorphisme qui élève toute racine m-ième de l'unité à la puissance ℓ ($\ell > 0$) ; on a donc :

$$\left(\frac{\mathbb{Q}(m)/\mathbb{Q}}{(a)}\right) = \sigma_{|a|,\mathbb{Q}(m)}$$

pour tout $a \in \mathbb{Q}^\times$, $(a,m) = 1$. Le noyau dans I_m de l'application d'Artin $I_m \to G_m$ est donc le rayon qui correspond à $\mathbb{Q}(m)$ (lequel devrait se noter $\mathbb{Q}(m\infty)$ puisque la place à

l'infini peut se ramifier) : c'est

$$R_{m\infty} = \{(u) \in I_m,\ u \equiv 1 \bmod m\infty\} = \{(u) \in I_m,\ u \equiv 1 \bmod m \text{ et } u > 0\};$$

or on vérifie facilement que l'on a l'isomorphisme canonique :

$$I_m/R_{m\infty} \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*$$
$$(a)R_{m\infty} \longrightarrow \mid a \mid +m\mathbb{Z}.$$

Ceci élucide le cas particulier de $\mathbb{Q}$, concernant la définition du symbole d'Artin, et nous utiliserons indifféramment les notations $\sigma_{|a|,F}$ ou $\left(\frac{F/\mathbb{Q}}{(a)}\right)$. On note à ce sujet que $\sigma_{-1,\mathbb{Q}(m)}$ est la restriction à $\mathbb{Q}(m)$ de la conjugaison complexe et peut s'écrire par exemple $\left(\frac{\mathbb{Q}(m)/\mathbb{Q}}{(m-1)}\right)$ comme symbole d'Artin usuel.

(ii) Si S est un ensemble de nombres premiers, on désigne par $\mathbb{Q}(S)$ la réunion des corps $\mathbb{Q}(m)$, lorsque m parcourt le sous-monoïde multiplicatif de $\mathbb{N} - \{0\}$:

$$\mathbb{N}_S = \{m = \prod_{\ell \in S} \ell^{n_\ell},\ n_\ell \geq 0,\ n_\ell \text{ presque tous nuls}\}. \tag{1.1.1}$$

(1.1.2) On désigne par G_S le groupe $Gal(\mathbb{Q}(S)/\mathbb{Q})$.

(1.2) **Remarques**. (i) Compte-tenu des utilisations ultérieures, nous supposons que toutes ces extensions abéliennes de $\mathbb{Q}$ sont vues dans une clôture algébrique de $\mathbb{Q}$ contenue dans $\mathbb{C}_p$, relativement à un premier p fixé une fois pour toutes.

La conjugaison complexe reste alors définie sans ambiguité sur les corps abéliens puisque, par composition avec un isomorphisme des clôtures algébriques de $\mathbb{Q}$ dans $\mathbb{C}_p$ et de $\mathbb{Q}$ dans $\mathbb{C}_\infty = \mathbb{C}$, elle agit toujours par inversion des racines de l'unité.

(ii) D'après le corps de classes, $\mathbb{Q}(S)$ est aussi l'extension abélienne $S \cup \{\infty\}$ -ramifiée maximale de $\mathbb{Q}$, c'est-à-dire la réunion des extensions abéliennes finies $F/\mathbb{Q}$ dans lesquelles les places de $\mathbb{Q}$ n'appartenant pas à $S \cup \{\infty\}$ ne se ramifient pas.

(iii) Si $F/\mathbb{Q}$ est une extension abélienne finie de $\mathbb{Q}$, on rappelle que le conducteur au sens usuel f de F est l'entier m minimum tel que $F \subseteq \mathbb{Q}(m)$, et qu'un nombre premier ℓ est ramifié dans $F/\mathbb{Q}$ si et seulement si ℓ divise f ; de façon plus précise, le conducteur généralisé est f ou $f\infty$ selon que F est réel ou imaginaire, et f est la partie finie du conducteur, mais nous n'utiliserons le conducteur généralisé que lorsque ce sera indispensable.

(iv) Ne pas confondre les notations $\mathbb{Q}(\{p\})$ et $\mathbb{Q}(p)$.
A ce sujet on pourra aussi écrire $\mathbb{Q}(m) = \mathbb{Q}(\mu_m)$ où μ_m est le groupe des racines m-ièmes de l'unité (dans $\mathbb{C}_p$); on a alors ici $\mathbb{Q}(\{p\}) = \mathbb{Q}(\mu_{p^\infty})$, où $\mu_{p^\infty} = \cup_{n \geq 0} \mu_{p^n}$.

(v) On notera enfin que pour $S = \emptyset$ on a $\mathbb{Q}(\emptyset) = \mathbb{Q}$, mais que pour tout $S \neq \emptyset$, $\mathbb{Q}(S)$ est une extension infinie imaginaire de $\mathbb{Q}$.

(1.3) **Théorème**. Le groupe $G_S = Gal(\mathbb{Q}(S)/\mathbb{Q})$ est un groupe profini canoniquement isomorphe à $\prod_{\ell \in S} \mathbb{Z}_\ell^*$ (algébriquement et topologiquement) ; cet homéomorphisme, noté N_S, est l'application qui à un $\mathbb{Q}$-automorphisme σ de $\mathbb{Q}(S)$ associe l'élément $a = (a_\ell)_{\ell \in S}$, où $a_\ell = (a_{\ell,n})_n \in \varprojlim_n (\mathbb{Z}/\ell^n\mathbb{Z})^*$ est défini par $\sigma(\zeta_{\ell^n}) = \zeta_{\ell^n}^{a_{\ell,n}}$ pour tout $\zeta_{\ell^n} \in \mu_{\ell^n}$, $n \geq 0$.

démonstration

D'après les résultats généraux de la théorie de Galois infinie (cf.(I.3.7)), et par le fait (théorème de Kronecker-Weber si l'on veut) que l'ensemble des corps $\mathbb{Q}(m)$, $m \in \mathbb{N}_S$, est une partie cofinale à l'ensemble $\mathcal{F}_S$ des extensions finies F de $\mathbb{Q}$ dans $\mathbb{Q}(S)$, on a

$$\begin{aligned} G_S &= \varprojlim_{m \in \mathbb{N}_S} G_m \\ &\simeq \varprojlim_{m \in \mathbb{N}_S} (\mathbb{Z}/m\mathbb{Z})^*, \end{aligned}$$

où $\mathbb{N}_S$ (cf.(1.1.1)) est ordonné via la relation de divisibilité, la relation $m \mid m'$ étant équivalente à l'inclusion $\mathbb{Q}(m) \subseteq \mathbb{Q}(m')$.
L'isomorphisme de systèmes projectifs (cf.(I.3.4)) se résume ici par la commutativité des diagrammes suivants (où $m \mid m'$) :

$$\begin{array}{ccccc} G_{m'} & \longrightarrow & (\mathbb{Z}/m'\mathbb{Z})^* & & a + m'\mathbb{Z} \\ \text{restriction} \downarrow & & \downarrow & & \downarrow \\ G_m & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^* & & a + m\mathbb{Z} \end{array}$$

les flèches horizontales étant les inverses des applications d'Artin sur $\mathbb{Q}(m')$ et $\mathbb{Q}(m)$, les flèches verticales étant les homomorphismes de transition attendus.

Ecrivons alors

$$(1.3.1) \qquad (\mathbb{Z}/m\mathbb{Z})^* \simeq \prod_{\ell \in S} (\mathbb{Z}/\ell^{n_\ell})^*, \text{où } m = \prod_{\ell \in S} \ell^{n_\ell} \in \mathbb{N}_S;$$

par un argument déjà utilisé au chapitre I, on a

$$\begin{aligned} \varprojlim_{m \in \mathbb{N}_S} (\mathbb{Z}/m\mathbb{Z})^* &\simeq \prod_{\ell \in S} \varprojlim_{n \geq 0} (\mathbb{Z}/\ell^n\mathbb{Z})^* \\ &= \prod_{\ell \in S} \mathbb{Z}_\ell^*. \end{aligned}$$

On en déduit alors l'expression de N_S.

(1.3.2) **Remarques.** (i) Supposons S fini. Si $a \in \mathbb{Z}$, $(a, S) = 1$, l'élément $(\sigma_{a,F})_F$, $F \in \mathcal{F}_S$, définit un élément de G_S que l'on appelle encore le symbole d'Artin de a, que l'on note σ_a ou $\sigma_{a,\mathbb{Q}(S)}$ et qui est égal à $\left(\frac{\mathbb{Q}(S)/\mathbb{Q}}{(a)}\right)$ lorsque $a > 0$. Il est clair que l'on a alors $N_S(\sigma_a) = (a)_{\ell \in S}$ (image diagonale de a dans $\prod_{\ell \in S} \mathbb{Z}_\ell^*$), et par conséquent, puisque $\mathbb{Z}$ est dense dans ce produit fini, l'ensemble des σ_a, $a \in \mathbb{Z}$, $(a, S) = 1$, est dense dans G_S (on peut même se restreindre aux $a > 0$).

(ii) Si S n'est pas fini, 2 cas se présentent : si S est l'ensemble $\mathbb{P}$ de tous les nombres premiers, la condition $(a, S) = 1$ donne $a = \pm 1$, ce qui définit l'identité et la conjugaison

complexe ; si $\mathbb{P} - S \neq \emptyset$, la condition $(a, S) = 1$ donne un ensemble infini de valeurs mais qui n'est pas nécessairement dense dans $\prod_{\ell \in S} \mathbb{Z}_\ell^*$.

(iii) Si l'on a $U \subseteq S$, on a donc $\mathbb{Q}(U) \subseteq \mathbb{Q}(S)$, et par la théorie de Galois, il correspond à $\mathbb{Q}(U)$ le sous-groupe fermé $H = Gal(\mathbb{Q}(S)/\mathbb{Q}(U))$ de G_S. On a $\sigma \in H$ si et seulement si σ fixe tout élément de $\mathbb{Q}(U)$, donc fixe μ_d pour tout $d \in \mathbb{N}_U$, donc si et seulement si, avec les notations de (1.3), $a_{\ell,n} \equiv 1 \bmod \ell^n$ pour tout $\ell \in U$ et tout $n \geq 0$, autrement dit si la composante a_ℓ de $N_S\, \sigma$ dans $\prod_{\ell \in S} \mathbb{Z}_\ell^*$ est 1 pour tout $\ell \in U$. D'où :

$$H \simeq N_S\, H = \prod_{\ell \in U} \mathbb{Z}_\ell^* \left(\text{vu comme sous} - \text{groupe de } \prod_{\ell \in S} \mathbb{Z}_\ell^*\right).$$

(1.4) **Proposition**. Le corps $\mathbb{Q}(S)$ est le composé direct sur $\mathbb{Q}$ des corps $\mathbb{Q}(\{\ell\}), \ell \in S$.

Ceci résulte du fait que pour tout $m \in \mathbb{N}_S$, $m = \prod_{\ell \in S} \ell^{n_\ell}$, $\mathbb{Q}(m)$ est le composé direct sur $\mathbb{Q}$ des corps $\mathbb{Q}(\ell^{n_\ell})$: ceci se voit au moyen de la ramification (entre autre) car ℓ est totalement ramifié dans $\mathbb{Q}(\ell^{n_\ell})/\mathbb{Q}$ et cette extension est non ramifiée en dehors de $\ell \cup \{\infty\}$.

(1.5) **Remarques**. (i) D'après (1.3.2), (iii), et (1.4), pour tout $\ell \in S$, $\mathbb{Q}(S)$ est le composé direct sur $\mathbb{Q}$ de $\mathbb{Q}(\{\ell\})$ et de $\mathbb{Q}(S - \{\ell\})$.Dans l'isomorphisme de (1.3), $Gal(\mathbb{Q}(S)/\mathbb{Q}(S - \{\ell\}))$ correspond à $\mathbb{Z}_\ell^*$ et $Gal(\mathbb{Q}(S)/\mathbb{Q}(\{\ell\}))$ à $\prod_{q \in S - \{\ell\}} \mathbb{Z}_q^*$.

(ii) On rappelle que l'on a les décompositions suivantes :

(α) Si $\ell \neq 2$, alors $\mathbb{Z}_\ell^* = \mu_{\ell-1} \oplus (1 + \ell\mathbb{Z}_\ell)$, où $1 + \ell\mathbb{Z}_\ell$ est un $\mathbb{Z}_\ell$-module sans torsion isomorphe (via le logarithme ℓ-adique) à $\mathbb{Z}_\ell$ et où $\mu_{\ell-1}$ est ici vu dans $\mathbb{C}_\ell$;

(β) Si $\ell = 2$, alors $\mathbb{Z}_2^* = \mu_2 \oplus (1 + 4\mathbb{Z}_2)$, où de même $1 + 4\mathbb{Z}_2 \simeq \mathbb{Z}_2$ et $\mu_2 = \{\pm 1\}$.

(1.6) **Définition**. Si S est l'ensemble $\mathbb{P}$ de tous les nombres premiers, $\mathbb{Q}(\mathbb{P})$ est l'extension abélienne maximale de $\mathbb{Q}$ dans $\mathbb{C}_p$ et on a $G_{\mathbb{P}} \simeq \widehat{\mathbb{Z}}^*$, groupe des éléments inversibles de l'anneau $\widehat{\mathbb{Z}}$ (cf.(1.3) et (I.3.6)). Le corps $\mathbb{Q}(\mathbb{P})$ se note plus simplement $\mathbb{Q}^{ab}$ et le groupe $G_{\mathbb{P}}$ se note G^{ab}.

(1.7) **Remarques**. (i) On notera à ce sujet que

$$\widehat{\mathbb{Z}}^* \simeq \prod_{\ell \in \mathbb{P}} \mathbb{Z}_\ell^* = \mu_2 \times (1 + 4\mathbb{Z}_2) \prod_{\ell \neq 2} \mu_{\ell-1} \times (1 + \ell\mathbb{Z}_\ell)\ ,$$

donc que l'on a :

$$G^{ab} \simeq \mu_2 \prod_{\ell \neq 2} \mu_{\ell-1} \times \prod_{\ell \in \mathbb{P}} \mathbb{Z}_\ell\ .$$

Autrement dit, G^{ab} est un exemple de groupe profini abélien qui pour tout premier p a un p-Sylow $G^{ab}(p)$ dont le sous-groupe de $\mathbb{Z}_p$-torsion n'est pas de type fini (car d'après le théorème de Dirichlet, il y a une infinité de premiers ℓ tels que $\ell \equiv 1 \bmod p$, i.e. où $|\, \mu_{\ell-1}\, | \equiv 0 \bmod p$) mais dont le quotient $G^{ab}(p)/tor(G^{ab}(p))$ est isomorphe à $\mathbb{Z}_p$. Le groupe G^{ab}

vérifie donc, pour tout p, l'hypothèse (H_p) (cf.(III.2.4)) et admet des décompositions de la forme

$$G^{ab} = A \oplus \Gamma,\ \Gamma \simeq \mathbb{Z}_p,$$

pour lesquelles $A(p)$ est infini et de torsion.

(ii) Si l'on suppose l'ensemble S fini, alors le p-Sylow $G_S(p)$ de G_S est fini si et seulement si $p \notin S$. Si $p \in S$, on peut décomposer G_S sous la forme

$$G_S = A_S \oplus \Gamma,\ \Gamma \simeq \mathbb{Z}_p,\ A_S(p) \text{ fini.}$$

Par exemple, on peut poser :

$$\begin{aligned} A_S &= Gal(\mathbb{Q}(S)/\mathbb{Q}_\infty) \text{ (cf.(2.1) ci} - \text{après)}, \\ \Gamma &= Gal(\mathbb{Q}(S)/\mathbb{Q}(S - \{p\})\mathbb{Q}(\mu_p)) \text{ si } p \neq 2, \\ \Gamma &= Gal(\mathbb{Q}(S)/\mathbb{Q}(S - \{2\})\mathbb{Q}(\mu_4)) \text{ si } p = 2. \end{aligned}$$

2.— Caractères remarquables de G_S.

Fixons un nombre premier p. D'une manière générale nous indiquerons entre parenthèses les modifications qu'implique en principe le cas $p = 2$; cependant, dans la plupart des cas nous utilisons la notation classique $q = p$ (resp. 4) selon que p est impair ou non et nous désignons par $\varphi(q) = p - 1$ (resp. 2) le nombre $|\ (\mathbb{Z}/q\mathbb{Z})^*\ |$.

D'après (1.3), on a $G_{\{p\}} \simeq \mathbb{Z}_p^* = \mu_{\varphi(q)} \oplus (1 + q\mathbb{Z}_p)$.

(2.1) **Définition**. Le sous-corps de $\mathbb{Q}(\{p\})$ fixe par $\mu_{\varphi(q)}$ se note $\mathbb{Q}_\infty$ et s'appelle la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}$; on a $Gal(\mathbb{Q}_\infty/\mathbb{Q}) \simeq \mathbb{Z}_p$.

(2.2) **Remarque**. On vérifie que $\mathbb{Q}_\infty$ est la réunion des corps $\mathbb{Q}_n$, de degrés p^n sur $\mathbb{Q}$, $n \geq 0$, définis ainsi : pour $p \neq 2$, $\mathbb{Q}_n$ est l'unique extension cyclique de degré p^n contenue dans $\mathbb{Q}(p^{n+1})$; pour $p = 2$, $\mathbb{Q}_n$ est le sous-corps réel maximal de $\mathbb{Q}(4 \times 2^n)$, également cyclique de degré 2^n sur $\mathbb{Q}$. Enfin $\mathbb{Q}(\{p\}) = \mathbb{Q}_\infty\mathbb{Q}(q)$ comme composé direct sur $\mathbb{Q}$.

(2.3) **Définition**. Soit S un ensemble quelconque de nombres premiers contenant p. On définit les 2 caractères suivants de G_S (on dira aussi des caractères du corps $\mathbb{Q}(S)$) :

(i) $\omega_p = \omega$, dit le caractère de Teichmüller pour p, qui est le composé :

$$G_S \xrightarrow{N_S} \prod_{\ell \in S} \mathbb{Z}_\ell^* \longrightarrow \mathbb{Z}_p^* \longrightarrow \mu_{\varphi(q)}\ ;$$

(ii) $\langle\ \rangle_p = \langle\ \rangle$, qui est le composé :

$$G_S \xrightarrow{N_S} \prod_{\ell \in S} \mathbb{Z}_\ell^* \longrightarrow \mathbb{Z}_p^* \longrightarrow 1 + q\mathbb{Z}_p\ .$$

(2.4) **Remarque.** On a $\omega\langle\ \rangle = N$, où $N = N_p$ est la projection

$$G_S \to \mathbb{Z}_p^*$$

et aussi le composé

$$G_S \longrightarrow G_{\{p\}} \overset{N_{\{p\}}}{\longrightarrow} \mathbb{Z}_p^* .$$

Par conséquent, N a pour noyau l'image de $\prod_{\ell \in S-\{p\}} \mathbb{Z}_\ell^*$ dans G_S, c'est-à-dire $Gal(\mathbb{Q}(S)/\mathbb{Q}(\{p\}))$ (cf.(1.5), (i)) ; il en résulte que ω est un caractère de $\mathbb{Q}(p)$ (d'ordre $\varphi(q)$), que $\langle\ \rangle$ est un caractère d'ordre p^∞ de $\mathbb{Q}_\infty$, et que N est un caractère de $\mathbb{Q}(\{p\})$.

3.— Distributions de Stickelberger.

Fixons un nombre premier p ainsi qu'un ensemble fini S de nombres premiers (contenant ou non p). Soit $\mathcal{F}'_S \subset \mathcal{F}_S$ l'ensemble des extensions finies de $\mathbb{Q}$ dans $\mathbb{Q}(S)$ qui ne sont pas dans $\mathbb{Q}(U)$, pour tout sous-ensemble strict U de S. On notera que $\mathcal{F}'_S$ est cofinale par rapport à $\mathcal{F}_S$.

(3.1) **Remarque.** On a $F \in \mathcal{F}'_S$ si et seulement si le conducteur f de F est divisible par tous les éléments de S et seulement eux.
A ce sujet, il est commode d'introduire (cf.(1.1.1)) :

(3.1.1) $$\mathbb{N}'_S = \{m \in \mathbb{N}_S,\ m \equiv 0 \bmod \ell \text{ pour tout } \ell \in S\}.$$

(3.2) **Définition.** Pour tout $F \in \mathcal{F}'_S$, on pose

$$\rho_F = \sum_{a \in [1,f]'} \Big(-\frac{a}{f} + \frac{1}{2}\Big)\sigma_{a,F}^{-1} ,$$

où $f \in \mathbb{N}'_S$ est le conducteur de F, où $[1,f]' = \{a \in \mathbb{Z},\ 1 \leq a \leq f \text{ et } (a,f) = 1\}$, et où $\sigma_{a,F}$ est la restriction à F de $\sigma_{a,\mathbb{Q}(S)}$ (cf.(1.3.2)).

(3.2.1) **Remarque.** On notera que l'on a choisi de relever $(\mathbb{Z}/f\mathbb{Z})^*$ dans l'intervalle $[1,f]'$ et non $[0,f[$ qui peut sembler plus naturel ; or nous pensons, en dépit des habitudes prises dans la littérature, qu'il faut utiliser l'intervalle $[1,f]'$ (d'ailleurs égal à $[0,f[$ pour $f > 1$) car pour $f = 1$, on trouve $\rho_{\mathbb{Q}} = -\frac{1}{2}$ et non la valeur inacceptable $\frac{1}{2}$).
On peut (peut-être) s'en convaincre en se reportant à (1-1), (i), où l'isomorphisme $I_f/R_{f\infty} \simeq (\mathbb{Z}/f\mathbb{Z})^*$ envoie (a) mod $R_{f\infty}$ sur $\mid a \mid$ mod $f\mathbb{Z}$; or dans I_f l'idéal nul n'est pas considéré (et pour $f = 1$ il est bien clair que dans $I_1/R_\infty = I_1/I_1$, l'image de (1) conduit canoniquement au représentant $1\cdots$) et on sait que le corps de classes général traite les groupes $I_f/R_{f\infty}$, la version $(\mathbb{Z}/f\mathbb{Z})^*$ ne se généralisant pas.

(3.3) **Proposition.** On a

$$(\rho_F)_{F \in \mathcal{F}'_S} \in \varprojlim_F \mathbb{Q}[G_F], \text{ où } G_F = Gal(F/\mathbb{Q}) .$$

(3.3.1) **Remarque**. On notera que F parcourt $\mathcal{F}_S'$ et non $\mathcal{F}_S$; on verra au §4 que pour $F \subset \mathbb{Q}(U)$, $U \subset S$, $U \neq S$, ρ_F n'est pas la restriction des $\rho_{F'}$, $F' \in \mathcal{F}_S'$, mais les $\rho_{F',F}$ sont des multiples de ρ_F dans $\mathbb{Q}[G_F]$; autrement dit, on peut voir les éléments ρ_F comme les éléments de Stickelberger primitifs.

On remarque que, par définition, on a

$$\rho_F = \rho_{\mathbb{Q}(f),F}$$

par restriction de $\mathbb{Q}(f)$ à F ; par conséquent, il suffit de vérifier la cohérence au niveau des corps $\mathbb{Q}(f) \in \mathcal{F}_S'$, à savoir que $\rho_{\mathbb{Q}(f'),\mathbb{Q}(f)} = \rho_{\mathbb{Q}(f)}$ dès que f, $f' \in \mathcal{N}_S'$, f divisant f' : Soient F, $F' \in \mathcal{F}_S'$, $F \subseteq F'$, F (resp. F') de conducteur f (resp. f'), on a donc $f \mid f'$ et si l'on suppose que $\rho_{\mathbb{Q}(f'),\mathbb{Q}(f)} = \rho_{\mathbb{Q}(f)}$, il vient :

$$\begin{aligned}\rho_{F',F} = \left(\rho_{\mathbb{Q}(f'),F'}\right)_F &= \rho_{\mathbb{Q}(f'),F} \\ &= \left(\rho_{\mathbb{Q}(f'),\mathbb{Q}(f)}\right)_F = \rho_{\mathbb{Q}(f),F} = \rho_F\ .\end{aligned}$$

Enfin, comme dernière réduction du problème, il suffit de prouver la cohérence lorsque $f' = \ell f$, $\ell \in S$.

On a $\rho_{\mathbb{Q}(\ell f),\mathbb{Q}(f)} = \sum_{a \in\ [1,\ell f]'} \left(\frac{-a}{\ell f} + \frac{1}{2}\right) \sigma^{-1}_{a,\mathbb{Q}(f)}$.

Pour $a \in [1,\ell f]$, posons $a = \lambda f + b$, $1 \leq b \leq f$, $0 \leq \lambda < \ell$; puisque $\ell \mid f$ et que $\mathbb{Q}(f) \in \mathcal{F}_S'$ (cf. (2.1)), on a $(b,S) = 1$ si et seulement si $(a,S) = 1$, par conséquent $a \in [1,\ell f]'$ si et seulement si $b \in [1,f]'$ et $\lambda \in [0,\ell[$. D'où :

$$\begin{aligned}\rho_{\mathbb{Q}(\ell f),\mathbb{Q}(f)} &= \sum_{\lambda,b} \left(-\frac{\lambda f + b}{\ell f} + \frac{1}{2}\right) \sigma^{-1}_{b,\mathbb{Q}(f)} \\ &= \sum_{b \in\ [1,f]'} \sum_{\lambda \in\ [0,\ell[} \left(-\frac{\lambda}{\ell} - \frac{b}{\ell f} + \frac{1}{2}\right) \sigma^{-1}_{b,\mathbb{Q}(f)}\ ;\end{aligned}$$

on a $\sum_{\lambda \in\ [0,\ell[} \left(-\frac{\lambda}{\ell} - \frac{b}{\ell f} + \frac{1}{2}\right) = -\frac{\ell(\ell-1)}{2\ell} - \frac{b}{f} + \frac{\ell}{2} = -\frac{b}{f} + \frac{1}{2}$,

d'où

$$\rho_{\mathbb{Q}(\ell f),\mathbb{Q}(f)} = \sum_{b \in\ [1,f]'} \left(-\frac{b}{f} + \frac{1}{2}\right) \sigma^{-1}_{b,\mathbb{Q}(f)} = \rho_{\mathbb{Q}(f)}. \tag{3.3.2}$$

Le second résultat important est le suivant et concerne les ρ_F pour toute extension abélienne $F \in \mathcal{F}_S'$.

(3.4) **Proposition**. Supposons que $p \in S$, et soit $\sigma \in G_S$; alors on a :

$$(1 - N\sigma.\sigma_F^{-1})\rho_F \in \mathbb{Z}_p[G_F] \text{ pour tout } F \in \mathcal{F}_S' \text{ (cf.(2.4))}.$$

Fixons $F \in \mathcal{F}'_S$ et désignons par f le conducteur de F.
Approchons σ au moyen d'un symbole d'Artin de la forme σ_c, $c \in \mathbb{Z}$, $(c,S) = 1$ (cf. (1.3.2),(i)), de telle sorte que $\sigma_{c,\mathbb{Q}(f)} = \sigma_{\mathbb{Q}(f)}$; on a donc $N\sigma_c = c$ et $N\sigma \equiv c \bmod f\mathbb{Z}_p$, d'où $(c - N\sigma)\left(-\frac{a}{f} + \frac{1}{2}\right) \in \mathbb{Z}_p$ pour tout a (car si $p = 2$, f est pair) ; il suffit donc de vérifier que

$$(1 - c\sigma_{c,F}^{-1})\rho_F \in \mathbb{Z}_p[G_F]\ . \tag{3.5}$$

On a $(1 - c\sigma_{c,F}^{-1})\rho_F = \sum_{a \in [1,f]'} \left(-\frac{a}{f} + \frac{1}{2}\right)\sigma_{a,F}^{-1} - \sum_{a \in [1,f]'} \left(\frac{-ac}{f} + \frac{c}{2}\right)\sigma_{ac,F}^{-1}$.
Pour tout $a \in [1,f]$, posons $ac = rf + b$, $1 \leq b \leq f$, $r \in \mathbb{Z}$; on a $(a,S) = 1$ si et seulement si $(b,S) = 1$, et lorsque a décrit $[1,f]'$, b décrit $[1,f]'$ aussi, et $r = r_b^c$ ne dépend que de b et c ; plus précisément, si $b \in [1,f]'$, on a

$$r_b^c = \frac{1}{f}\left(\left[\frac{b}{c}\right]_f c - b\right), \tag{3.5.1}$$

où $\left[\frac{b}{c}\right]_f$ désigne l'unique représentant entier de $\frac{b}{c}$ modulo f dans $[1,f]'$. Il vient donc

$$\begin{aligned}(1 - c\sigma_{c,F}^{-1})\rho_F &= \sum_{a \in [1,f]'} \left(-\frac{a}{f} + \frac{1}{2}\right)\sigma_{a,F}^{-1} + \sum_{a \in [1,f]'} \left(r_b^c + \frac{b}{f} - \frac{c}{2}\right)\sigma_{b,F}^{-1} \\ &= \sum_{b \in [1,f]'} \left(r_b^c + \frac{1-c}{2}\right)\sigma_{b,F}^{-1}\end{aligned}$$

qui est bien dans $\mathbb{Z}_p[G_F]$ puisque si $p = 2$, c est forcément impair et $\frac{1-c}{2}$ entier.

Les propositions (3.4) et (3.5) nous permettent de mettre en évidence des distributions sur G_S (dites de Stickelberger, compte-tenu du fait que les ρ_F sont appelés souvent les éléments de Stickelberger). Leur nature dépend fortement du fait que $p \in S$ ou non, ainsi que de la parité de p.

Pour simplifier, nous notons Λ_S, Δ_S, Δ'_S les $\mathbb{Z}_p$-algèbres Λ_{G_S}, Δ_{G_S}, Δ'_{G_S} (cf. (II.6.3.4)).

(3.6) **Théorème**. Soit p un nombre premier fixé et soit S un ensemble fini de nombres premiers ; on considère $\rho = (\rho_F)_{F \in \mathcal{F}'_S}$, où $\rho_F = \sum_{a \in [1,f]'} \left(-\frac{a}{f} + \frac{1}{2}\right)\sigma_{a,F}^{-1}$ (cf. (3.2), (3.3)), où f est le conducteur de F.

(i) Si $p \notin S$ et si $p \neq 2$, ρ définit une $\mathbb{Z}_p$-mesure notée $St_S \in \Lambda_S$.

(ii) Si $p = 2 \notin S$, ρ définit la $\mathbb{Z}_2$-distribution $St_S \in \frac{1}{2}\Lambda_S$.

(iii) Si $p \in S$, pour tout $\tau \in G_S$ tel que $\langle\tau\rangle \neq 1$, ρ définit une distribution $St_S \in \Delta'_S$ de la forme $\frac{\nu_S^\tau}{\delta^\tau}$, $\delta^\tau = 1 - N\tau.\tau^{-1}$, $\nu_S^\tau \in \Lambda_S$, telle que $\nu_{S,F}^\tau = \delta_F^\tau \rho_F$ pour tout $F \in \mathcal{F}'_S$. En outre, si $\tau = \sigma_c$, $c \in \mathbb{Z}$, $c \neq \pm 1$, alors $\nu_{S,F}^\tau = \nu_{S,F}^c = \sum_{a \in [1,f]'} R_a^c \sigma_{a,F}^{-1}$, où $R_a^c = r_a^c + \frac{1-c}{2}$ avec $r_a^c = \frac{1}{f}\left(\left[\frac{a}{c}\right]_f c - a\right) \in \mathbb{Z}$.

démonstration

Les points (i) et (ii) résultent trivialement de l'expression même de $\rho_F \in \mathbb{Z}_p[G_F]$ (resp. $\frac{1}{2}\mathbb{Z}_2[G_F]$) et de (3.3).

Le point (iii) est un peu plus subtil :

Posons $\nu_F^\tau = \delta_F^\tau \rho_F$ pour tout $F \in \mathcal{F}_S'$; comme on a trivialement

$$(\delta_F^\tau)_F \in \varprojlim_F \mathbb{Z}_p[G_F] \subseteq \varprojlim_F \mathbb{Q}_p[G_F] ,$$

il résulte de (3.3) que $(\nu_F^\tau)_F \in \varprojlim_F \mathbb{Q}_p[G_F]$. Comme $\nu_F^\tau \in \mathbb{Z}_p[G_F]$ pour tout $F \in \mathcal{F}_S'$ d'après (3.4), il en résulte que $(\nu_F^\tau)_F \in \varprojlim_F \mathbb{Z}_p[G_F]$; d'où l'existence de $\nu_S^\tau \in \Lambda_S$ telle que $\nu_{S,F}^\tau = \nu_F^\tau = \delta_F^\tau \rho_F$ pour tout $F \in \mathcal{F}_S'$ car il suffit de poser :

$$St_S = \frac{\nu_S^\tau}{\delta^\tau}$$

à condition de vérifier que pour tout $F \in \mathcal{F}_S'$, δ_F^τ est non nul et non diviseur de 0 dans $\mathbb{Z}_p[G_F]$, ce qui résulte du choix de τ ($\langle\tau\rangle \neq 1$) compte-tenu du résultat suivant :

(3.6.1) **Lemme.** Les conditions suivantes sont équivalentes (lorsque $p \in S$) :

(i) $\delta^\tau = 1 - N\tau.\tau^{-1}$ est nul ou diviseur de 0 dans Λ_S ;

(ii) il existe une extension finie F_0 de $\mathbb{Q}$ dans $\mathbb{Q}(S)$ telle que $\delta_{F_0}^\tau$ est nul ou diviseur de 0 dans $\mathbb{Z}_p[G_{F_0}]$;

(iii) $N\tau$ est une racine de l'unité dans $\mathbb{Z}_p^*$ (i.e. $\langle\tau\rangle = 1$).

(i) $\Rightarrow$ (ii). Si $\delta^\tau = 0$, tout F_0 convient. Si $\delta^\tau \neq 0$ est diviseur de 0 dans Λ_S, il existe $\alpha = (\alpha_F)_F \in \varprojlim \mathbb{Z}_p[G_F]$, $\alpha \neq 0$, tel que $\delta_F^\tau \alpha_F = 0$ pour tout $F \in \mathcal{F}_S$; comme $\alpha \neq 0$, il existe $F_0 \in \mathcal{F}_S$ pour lequel $\alpha_{F_0} \neq 0$, donc $\delta_{F_0}^\tau$ est nul ou diviseur de 0 dans $\mathbb{Z}_p[G_{F_0}]$.

(ii) $\Rightarrow$ (iii). La transformée de Fourier dans $\mathbb{C}_p[G_{F_0}]$ montre qu'il existe $\chi \in X_{G_{F_0}}$ tel que $\langle\chi, \delta_{F_0}^\tau\rangle = 0$, soit $1 - N\tau.\chi(\tau_{F_0}) = 0$, ce qui conduit à $N\tau = \chi(\tau_{F_0}) \in \mathbb{Z}_p^*$ et est racine de l'unité.

(iii) $\Rightarrow$ (i). Considérons $\delta = 1 - \zeta\tau^{-1}$, avec $\zeta = N\tau \in \mu_q$, et considérons une décomposition de G_S sous la forme

$$G_S = B \oplus M \oplus \Gamma ,$$

de telle sorte que dans l'isomorphisme N_S (cf. (1.3)), B, M, Γ correspondent respectivement à $\prod_{\ell \in S-\{p\}} \mathbb{Z}_\ell^*$, $\mu_{\varphi(q)}$, $1 + q\mathbb{Z}_p$. On peut écrire :

$$\tau = bt\gamma,\ b \in B,\ t \in M,\ \gamma \in \Gamma ;$$

comme $N\tau = \zeta$ est d'ordre fini, que $Nb = 1$, et que Nt est d'ordre fini, $N\gamma$ doit être d'ordre fini, donc égal à 1, auquel cas $\gamma = 1$ et $\tau = bt$ avec $N\tau = Nt = \zeta$.

Comme $B(p)$ est fini, considérons la mesure de Haar α_B sur B, qui est non nulle (cf. (II.4.3)), et posons, n étant l'ordre commun de ζ et t :

$$\alpha = \alpha_B \sum_{i=0}^{n-1} \zeta^i b^{-i} t^{-i},$$

qui est dans Λ_S et qui est non nulle car on a aussi

$$\alpha = \alpha_B \sum_{i=0}^{n-1} \zeta^i t^{-i} \in \Lambda_B[M]$$

qui est trivialement non nulle dans cette algèbre du groupe M.
Or

$$\begin{aligned}\alpha\delta &= \alpha_B(1-\zeta b^{-1}t^{-1}) \sum_{i=0}^{n-1} \zeta^i b^{-i} t^{-i} \\ &= \alpha_B(1-\zeta^n b^{-n} t^{-n}) = \alpha_B(1-b^{-n}) = 0.\end{aligned}$$

Ainsi $\delta = 1 - \zeta\tau^{-1}$ est nul ou diviseur de 0 dans Λ_S.

Ceci achève la démonstration de (3.6.1), donc de (3.6).

(3.6.2) **Remarques**. (i) Pour $S = \emptyset$, on a $\mathcal{F}_\emptyset = \{\mathbb{Q}\}$, d'où
$St_\emptyset = \rho_\mathbb{Q} = \sum_{a\in[1,1]'} (-\frac{a}{1} + \frac{1}{2})\sigma_{a,\mathbb{Q}}^{-1} = -\frac{1}{2}$, puisque $f = 1$ et qu'alors $[1,1]' = \{1\}$,

cas qui est susceptible du cas (i) ou (ii) de (3.6) selon que $p \neq 2$ ou $p = 2$.

(ii) D'une manière générale, si μ est un diviseur de 0 (non nul) dans la $\mathbb{Z}_p$-algèbre Λ_G d'un groupe profini commutatif G, μ_H est nul ou diviseur de 0 dans $\mathbb{Z}_p[G/H]$ pour tout $H \in \Omega_G$ et en outre μ_H est diviseur de 0 (non nul) pour tout H assez petit : en effet, soit $\lambda \in \Lambda_G$, $\lambda \neq 0$, telle que $\lambda\mu = 0$; cette relation implique $\lambda_H\mu_H = 0$ pour tout $H \in \Omega_G$, d'où le fait que λ_H soit nul ou diviseur de 0 dans $\mathbb{Z}_p[G/H]$; mais comme $\lambda \neq 0$, il existe $H_0 \in \Omega_G$ tel que $\lambda_{H_0} \neq 0$, auquel cas pour tout $H \subseteq H_0$ on a $\lambda_H \neq 0$.

4.— Propriétés eulériennes des distributions St_S.

Soit S un ensemble fini de nombres premiers contenant ou non p.

(4.1) **Définition**. Soient K et L des sous-corps quelconques de $\mathbb{Q}(S)$ tels que $K \subseteq L$; soient $G_K = Gal(K/\mathbb{Q})$, $G_L = Gal(L/\mathbb{Q})$ et posons $\Lambda_K = \Lambda_{G_K}$, $\Lambda_L = \Lambda_{G_L}$. Il existe une application naturelle

$$Res_{L,K} : \Lambda_L \to \Lambda_K$$

qui s'obtient à partir de la projection canonique $G_L \to G_K$, par $\mathbb{Z}_p$-linéarité, de $\mathbb{Z}_p[G_L]$ dans $\mathbb{Z}_p[G_K]$, puis par continuité (cf. (II.3.2)). Soit Δ_L' la sous-algèbre de $\Delta_L = \Delta_{G_L}$ formée des distributions $\frac{\nu}{\delta}$ pour lesquelles $Res_{L,F}(\delta)$ est non nul et non diviseur de 0 dans

Λ_F pour tout sous-corps F de L de degré fini (cf. (II.6.3.4)) ; alors $Res_{L,K}$ se prolonge canoniquement à Δ'_L, quel que soit $K \subseteq L$, par la formule

$$Res_{L,K}\left(\frac{\nu}{\delta}\right) = \frac{Res_{L,K}(\nu)}{Res_{L,K}(\delta)}.$$

(4.1.1) **Notations.** Pour tout sous-corps K de L et tout $\rho \in \Delta'_L$, on pose $Res_{L,K}(\rho) = \rho_K$; lorsque K est un corps de la forme $\mathbb{Q}(V)$, on pose $\rho_{\mathbb{Q}(V)} = \rho_V$ pour simplifier. Ceci est cohérent avec la notation St_V introduite en (3.6) et qui peut également se lire $St_{\mathbb{Q}(V)}$.

(4.1.2) **Remarque.** Lorsque K, L, $K \subseteq L$, sont des extensions finies de $\mathbb{Q}$, on a $\Delta'_L = \Delta_L = \mathbb{Q}_p[G_L]$ d'après (II.6.3) (de même pour K), et $Res_{L,K}$ coïncide avec l'application canonique $\mathbb{Q}_p[G_L] \to \mathbb{Q}_p[G_K]$.

(4.2) **Définition.** Soit L un sous-corps de $\mathbb{Q}(S)$. On pose

$$St_L = Res_{\mathbb{Q}(U),L}(St_U) = St_{U,L}\ ,$$

où U est le sous-ensemble minimum de S tel que $L \subseteq \mathbb{Q}(U)$ (définition primitive de la distribution de Stickelberger de L (cf. (3.3.1)).

On se propose essentiellement de calculer $St_{L,K}$, pour $K \subseteq L \subseteq \mathbb{Q}(S)$.

Désignons par U (resp.V) le sous-ensemble minimum de S tel que $L \subseteq \mathbb{Q}(U)$ (resp. $K \subseteq \mathbb{Q}(V)$) (ce sont les ensembles de nombres premiers ramifiés dans L (resp. K)).

On a donc :

$$St_{L,K} = St_{U,L,K} = St_{U,V,K} \text{ (cf.(4.1.1.))}.$$

On est donc ramené au calcul de $St_{U,V}$.

(4.3) **Proposition.** On a $St_{U,V} = St_V \prod_{\ell \in U-V} (1 - \sigma_{\ell,V}^{-1})$.

Par induction, il suffit de faire le calcul lorsque $U = V \cup \{\ell\}$, $\ell \notin V$.

(4.3.1) **Lemme.** Si $f \in \mathbb{N}'_V$, alors $f\ell \in \mathbb{N}'_U$ et on a :

$$\rho_{\mathbb{Q}(f\ell),\mathbb{Q}(f)} = \rho_{\mathbb{Q}(f)}(1 - \sigma_{\ell,\mathbb{Q}(f)}^{-1}).$$

On a $\rho_{\mathbb{Q}(f\ell),\mathbb{Q}(f)} = \sum_{a \in [1,f\ell]'} \left(-\frac{a}{f\ell} + \frac{1}{2}\right) \sigma_{a,\mathbb{Q}(f)}^{-1}$.

Pour tout $a \in [1, f\ell]$, posons $a = \lambda f + b$, $0 \leq \lambda < \ell$, $1 \leq b \leq f$; lorsque a parcourt $[1, f\ell]$, λ et b parcourent respectivement $[0, \ell[$, $[1, f]$; on a $(a, U) = 1$ si et seulement si :

(i) $(b, V) = 1$,

(ii) $\lambda f + b \not\equiv 0 \bmod \ell$.

Pour b fixé satisfaisant à (i), la condition (ii) élimine une valeur de λ et une seule, que l'on peut noter λ_b et qui est telle que :

(iii) $\lambda_b f + b = \ell n_b$ (on a alors $n_b \in [1, f]$).
Il vient :

$$\rho_{\mathbb{Q}(f\ell),\mathbb{Q}(f)} = \sum_{b\in[1,f]'} \sum_{\lambda\in[0,\ell[} \left(-\frac{\lambda}{\ell} - \frac{b}{f\ell} + \frac{1}{2}\right) \sigma^{-1}_{b,\mathbb{Q}(f)} - \sum_{b\in[1,f]'} \left(-\frac{\lambda_b f + b}{f\ell} + \frac{1}{2}\right) \sigma^{-1}_{b,\mathbb{Q}(f)}.$$

D'après les calculs effectués dans la preuve de (3.3), la $1^{ère}$ somme vaut $\rho_{\mathbb{Q}(f)}$; la seconde s'écrit :

$$\sum_{b\in[1,f]'} \left(-\frac{n_b}{f} + \frac{1}{2}\right)\sigma^{-1}_{b,\mathbb{Q}(f)} \ ;$$

or, lorsque b parcourt $[1, f]$, l'entier n_b parcourt le même intervalle et on a $(b, V) = 1$ si et seulement si $(n_b, V) = 1$, auquel cas n_b parcourt ici $[1, f]'$. La relation (iii) conduit à

$$\sigma_{b,\mathbb{Q}(f)} = \sigma_{\ell n_b,\mathbb{Q}(f)} = \sigma_{\ell,\mathbb{Q}(f)}\sigma_{n_b,\mathbb{Q}(f)} \ ;$$

d'où la seconde sommation

$$\sum_{a\in[1,f]'} \left(-\frac{a}{f} + \frac{1}{2}\right)\sigma^{-1}_{a,\mathbb{Q}(f)}\sigma^{-1}_{\ell,\mathbb{Q}(f)} = \rho_{\mathbb{Q}(f)}\sigma^{-1}_{\ell,\mathbb{Q}(f)} \ ,$$

d'où le lemme puis le résultat suivant :

(4.3.2) **Corollaire.** Pour tout $f \in \mathbb{N}'_V$ et pour tout $f' \in \mathbb{N}'_U$, $U = V \cup \{\ell\}$, f' multiple de f, on a

$$\rho_{\mathbb{Q}(f'),\mathbb{Q}(f)} = \rho_{\mathbb{Q}(f)}(1 - \sigma^{-1}_{\ell,\mathbb{Q}(f)}) \ .$$

Ceci étant, pour passer à la limite projective, on doit considérer $\nu^\tau_{\mathbb{Q}(f')} = \delta^\tau_{\mathbb{Q}(f')}\rho_{\mathbb{Q}(f')}$, pour $\tau \in G_U$ tel que δ^τ soit non nul et non diviseur de 0 dans Λ_U ; il vient alors

$$\begin{aligned}\nu^\tau_{\mathbb{Q}(f'),\mathbb{Q}(f)} &= \delta^\tau_{\mathbb{Q}(f)}\rho_{\mathbb{Q}(f'),\mathbb{Q}(f)} = \delta^\tau_{\mathbb{Q}(f)}\rho_{\mathbb{Q}(f)}(1 - \sigma^{-1}_{\ell,\mathbb{Q}(f)}) \\ &= \nu^\tau_{\mathbb{Q}(f)}(1 - \sigma^{-1}_{\ell,\mathbb{Q}(f)}) \ .\end{aligned}$$

On obtient alors dans les algèbres de mesures :

$$\nu^\tau_{U,V} = \nu^\tau_V(1 - \sigma^{-1}_{\ell,V}) \ ,$$

puis, au niveau distributions :

$$St_{U,V} = St_V(1 - \sigma^{-1}_{\ell,V}) \ ;$$

d'où la proposition (4.3) par induction.

On en déduit alors le calcul suivant déjà évoqué :

$$\begin{aligned} St_{L,K} &= St_{U,L,K} = St_{U,V,K} \\ &= St_{V,K} \prod_{\ell \in U-V} (1 - \sigma_{\ell,V}^{-1})_K \end{aligned}$$

soit

$$St_{L,K} = St_K \prod_{\ell \in U-V} (1 - \sigma_{\ell,K}^{-1}) \,. \tag{4.4}$$

(4.5) **Lemme.** Si le corps K est réel distinct de $\mathbb{Q}$, alors $St_K = 0$. On a $St_{\mathbb{Q}} = -\frac{1}{2}$.

Le cas de $St_{\mathbb{Q}}$ étant clair (cf. (3.6.2)), on suppose K réel, $K \neq \mathbb{Q}$; par conséquent $K \subseteq \mathbb{Q}(V)$ avec $V \neq \emptyset$ et $\mathbb{Q}(V)$ est un corps totalement imaginaire. On a donc $K \subseteq \mathbb{Q}(V)^+$, le sous-corps réel maximal de $\mathbb{Q}(V)$ et il suffit de calculer $St_{V,\mathbb{Q}(V)^+}$. Par analogie avec la preuve de (4.3), il suffit de calculer $\rho_{\mathbb{Q}(f),\mathbb{Q}(f)^+}$, $f \in \mathbb{N}_V'$, (on a donc $f \neq 1$).

Or on a $\rho_{\mathbb{Q}(f)} = \sum_{a \in [1,f]'} \left(-\frac{a}{f} + \frac{1}{2}\right) \sigma_{a,\mathbb{Q}(f)}^{-1}$; dans la restriction à $\mathbb{Q}(f)^+$, $\sigma_{a,\mathbb{Q}(f)^+} = \sigma_{f-a,\mathbb{Q}(f)^+}$ puisque $\sigma_{f-a,\mathbb{Q}(f)} = \sigma_{-1,\mathbb{Q}(f)} \sigma_{a,\mathbb{Q}(f)}$ et que $\sigma_{-1,\mathbb{Q}(f)^+}$ est l'identité ; comme $f - a = a$ n'a jamais lieu et que l'application $a \to f - a$ réalise une bijection de $[1,f]'$ sur $[0,f['$ qui est égal à $[1,f]'$ dès que $f \neq 1$, on obtient :

$$\begin{aligned} 2\rho_{\mathbb{Q}(f),\mathbb{Q}(f)^+} &= \sum_{a \in [1,f]'} \left(-\frac{a}{f} + \frac{1}{2} - 1 + \frac{a}{f} + \frac{1}{2}\right) \sigma_{a,\mathbb{Q}(f)^+}^{-1} \\ &= 0. \end{aligned}$$

D'où le fait que $St_{V,\mathbb{Q}(V)^+} = 0$, et le résultat.

En conclusion, on peut écrire le résultat final suivant :

(4.6) **Théorème.** Soient K, L, $K \subseteq L$, des sous-corps imaginaires de $\mathbb{Q}^{ab}$; on suppose que l'ensemble des nombres premiers ramifiés dans $L/\mathbb{Q}$ est fini. Alors on a, par restriction de Δ_L' à Δ_K' (cf. (4.1)) :

$$St_{L,K} = St_K \prod_{\ell} (1 - \sigma_{\ell,K}^{-1}) \,,$$

où ℓ parcourt l'ensemble des nombres premiers qui sont ramifiés dans $L/\mathbb{Q}$ mais non dans $K/\mathbb{Q}$.

(4.7) **Remarques.** (i) Si K est réel et L imaginaire, on a $St_{L,K} = 0$ comme on le vérifie facilement en reconsidérant (4.5) pour en déduire que $St_{L,L^+} = 0$ pour tout corps imaginaire L.

(ii) Supposons que $p \in S$ et considérons par exemple $U = S - \{p\}$; d'après (3.6), St_S est dans $\Delta_S' - \Lambda_S$ tandis que $St_U \in \Lambda_S$ (resp. $\frac{1}{2}\Lambda_S$ si $p = 2$) ; on a donc

$St_{S,U} = St_U(1 - \sigma_{p,U}^{-1}) \in \Lambda_S$ (resp.$\frac{1}{2}\Lambda_S$). Ceci est néanmoins cohérent pour les raisons suivantes : Ecrivons $St_S = \frac{\nu_S^\tau}{\delta^\tau}$, $\tau \in Gal(\mathbb{Q}(S)/\mathbb{Q}(U)) \simeq Gal(\mathbb{Q}(\{p\})/\mathbb{Q})$, de telle sorte que $N\tau = \zeta(1+q)$ où $o(\zeta) = \varphi(q)$; par restriction il vient $\delta_U^\tau = 1 - N\tau \in \mathbb{Z}_p$ et de façon précise $1 - N\tau \in \mathbb{Z}_p^*$ (resp. $2\mathbb{Z}_2^*$), ce qui donne bien le résultat attendu.

(iii) Au sujet des facteurs eulériens $E_{\ell,V} = 1 - \sigma_{\ell,V}^{-1}$, $V \subseteq U$, $\ell \in U - V$, si $p \in V$ (auquel cas $\ell \neq p$), l'involution de Mellin m que l'on utilisera au chapitre V, §2, permet d'écrire

$$m(E_{\ell,V}) = 1 - \ell^{-1}\sigma_{\ell,V}$$

qui est de la forme δ^τ avec $\tau = \sigma_{\ell,V}^{-1}$, et donc non nul et non diviseur de 0 dans Λ_V puisque $\langle\tau\rangle = \langle\ell\rangle \neq 1$.
Si $p \notin V$, le p-Sylow de G_V est fini et sa mesure de Haar $\alpha_V \neq 0$ vérifie $E_\ell \alpha_V = 0$, ce qui fait que $E_{\ell,V}$ est dans ce cas diviseur de 0 (les restrictions $E_{\ell,F}$ sont nulles si et seulement si F est contenu dans le corps de décomposition de ℓ dans $\mathbb{Q}(V)/\mathbb{Q}$).

(4.8) **Proposition**. Soit S un ensemble fini non vide de nombres premiers et posons $St_S = \frac{\nu_S^\tau}{\delta^\tau}$ (cf. (3.6)) ; alors il existe $\nu_S^{\tau+} \in \Lambda_S$, définie modulo $(1+\sigma_{-1,S})\Lambda_S$, telle que $\nu_S^\tau = (1-\sigma_{-1,S})\nu_S^{\tau+}$. On pose alors $St_S^+ = \frac{\nu_S^{\tau+}}{\delta^\tau}$ qui est donc définie modulo $(1+\sigma_{-1,S})(\delta^\tau)^{-1}\Lambda_S$.

Ecrivons par exemple $\nu_S^\tau = (\nu_F^\tau)_F$, où F parcourt l'ensemble des corps $\mathbb{Q}(f)$, $f \in \mathbb{N}_S'$ (ensemble cofinal à $\mathcal{F}_S$) ; on a donc $\nu_{F,F+}^\tau = 0$ d'après (4.7) ; or on vérifie facilement que, dans $\mathbb{Z}_p[G_F]$, une telle relation équivaut à l'existence de $\nu_F^{\tau+} \in \mathbb{Z}_p[G_F]$ telle que $\nu_F^\tau = (1 - \sigma_{-1,F})\nu_F^{\tau+}$. Considérons alors une famille de relèvements $\nu_F^{\tau+'} \in \mathbb{Z}_p[G_S]$; par compacité, on peut en extraire une suite convergente dans Λ_S dont la limite $\nu_S^{\tau+}$ est solution (non unique évidemment).

(4.9) **Remarque**. Cette propriété de parité est en particulier à l'origine du fait qu'il n'existe pas de fonctions L_p pour des caractères impairs. Il serait intéressant de définir $St_S^+ = \frac{\nu_S^{\tau+}}{\delta^\tau}$ de façon intrinsèque, auquel cas on pourrait espérer créer de nouvelles fonctions L_p. Dans cette direction, on a le résultat suivant lorsque $p \in S$:

(4.10) **Proposition**. Posons, pour tout $c \in \mathbb{Z}$, $(c,S) = 1$, $c \neq \pm 1$, $R_a^c = r_a^c + \frac{1-c}{2}$ (cf.(3.6),(iii)) ; alors on a

$$(1 - c\sigma_{c,F}^{-1})\rho_F = (1 - \sigma_{-1,F}) \sum_{a \in [1,\frac{f}{2}]'} R_a^c \sigma_{a,F}^{-1},$$

où $[1,\frac{f}{2}]' = \{a \in [1,\frac{f}{2}],\ (a,f) = 1\}$.

Les calculs conduisant à cette expression seront effectués en détail plus loin (cf. (V.1.3), (iv)).

5.— Caractères abéliens – Nombres de Bernoulli.

(5.1) **Définitions**. (i) Considérons G^{ab}, le groupe de Galois de l'extension abélienne maximale de $\mathbb{Q}$ dans $\mathbb{C}_p$, et soit $tor(X_{G^{ab}})$, noté $tor(X^{ab})$, le groupe des caractères d'ordre fini

de G^{ab}. Si $\chi \in tor(X^{ab})$, $Ker\chi$ fixe une extension cyclique de $\mathbb{Q}$ notée K_χ. On appelle alors conducteur de χ le conducteur f_χ de K_χ ; si le corps K_χ est réel (resp. imaginaire) on dit que χ est pair (resp. impair) et ceci se caractérise par la condition $\chi(\sigma_{-1}) = 1$ (resp. -1).

(ii) Soit f un multiple de f_χ; le caractère χ est toujours un caractère de $Gal(\mathbb{Q}(f)/\mathbb{Q})$, donc de $(\mathbb{Z}/f\mathbb{Z})^*$; l'application (notée encore χ par abus) :

$$\chi : \mathbb{Z} \to \mathbb{C}_p$$

définie par $\chi(a) = \chi(\sigma_{a,\mathbb{Q}(f)})$ si $(a,f) = 1$, $\chi(a) = 0$ sinon, s'appelle le caractère de Dirichlet modulo f déduit du caractère abélien χ. Si $f = f_\chi$, le caractère χ est dit primitif. On vérifie facilement que le conducteur f_χ d'un caractère de Dirichlet modulo f est le plus petit diviseur m de f tel que $\chi(a) = 1$ pour tout a modulo f, $(a,f) = 1$, tel que $a \equiv 1 \bmod m$ (i.e. on cherche le plus petit corps cyclotomique $\mathbb{Q}(m)$ tel que $Gal(\mathbb{Q}(f)/\mathbb{Q}(m)) \subseteq Ker\chi$).

Lorsque nous parlerons de caractère de Dirichlet, sans autre précision, il s'agira toujours de caractères primitifs. Si nécessaire, nous noterons χ' le caractère primitif associé au caractère χ.

(iii) On appelle fonction L de Dirichlet du caractère (de Dirichlet) χ, la fonction de variable complexe :

$$L(\chi, s) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}, \ \Re e(s) > 1.$$

Pour le caractère unité modulo 1 (noté χ_0), on obtient la fonction $\zeta_{\mathbb{Q}}(s)$ de Riemann qui admet en $s = 1$ un pôle simple de résidu 1.

(5.2) **Fonctions ζ partielles.** Soit f un entier ≥ 1, et soit χ un caractère de Dirichlet modulo f ; on peut écrire

$$\begin{aligned} L(\chi, s) = \sum_{n \geq 1} \frac{\chi(n)}{n^s} &= \sum_{\substack{n \geq 1 \\ (n,f)=1}} \frac{\chi(n)}{n^s} \\ &= \sum_{c \in (\mathbb{Z}/f\mathbb{Z})^*} \chi(c) \sum_{\substack{n \geq 1 \\ n \in c}} \frac{1}{n^s} \\ &= \sum_{c \in (\mathbb{Z}/f\mathbb{Z})^*} \chi(c)\ \zeta_f(c, s), \end{aligned}$$

où

$$\zeta_f(c,s) = \sum_{\substack{n \geq 1 \\ n \in c}} \frac{1}{n^s}, f \geq 1, c \in (\mathbb{Z}/f\mathbb{Z})^*, \tag{5.2.1}$$

est appelée la fonction ζ partielle de $\mathbb{Q}$ pour la classe c modulo f.

On a en particulier $\zeta_{\mathbb{Q}}(s) = \zeta_1(\mathbb{Z}, s)$ et on voit qu'il suffit de donner les propriétés de ces fonctions pour reconstituer celles des fonctions L de Dirichlet (notamment en ce qui concerne les questions de prolongement analytique).

On rappelle (cf. [L]) que $L(\chi, s)$ admet le développement eulérien infini suivant :

$$L(\chi, s) = \prod_{p \in \mathbb{P}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}, \ \Re e'(s) > 1, \tag{5.2.2}$$

où $\mathbb{P}$ est l'ensemble des nombres premiers ; il en résulte la formule importante suivante reliant $L(\chi, s)$, où χ est un caractère de Dirichlet modulo f, à $L(\chi', s)$, où χ' est le caractère primitif déduit de χ :

$$L(\chi, s) = \prod_{\ell \mid f, \ell \nmid f_\chi} \left(1 - \frac{\chi(\ell)}{\ell^s}\right) \cdot L(\chi', s), \tag{5.2.3}$$

formule qui reste valable pour les prolongements analytiques correspondants sur $\mathbb{C}$.

(5.3) **Définitions.** (i) On appelle nombres de Bernoulli généralisés $B_n(\chi)$, $n \geq 0$, χ caractère de Dirichlet modulo f, les nombres définis par le développement suivant dans $\mathbb{C}_p[[t]]$:

$$\sum_{a \in [1,f]'} \frac{\chi(a) t e^{at}}{e^{ft} - 1} = \sum_{n \geq 0} B_n(\chi) \frac{t^n}{n!}.$$

(ii) On définit également les polynomes de Bernoulli $\mathbb{B}_n(X)$ au moyen de l'identité dans $\mathbb{Q}[X][[t]]$:

$$\frac{te^{Xt}}{e^t - 1} = \sum_{n \geq 0} \mathbb{B}_n(X) \frac{t^n}{n!}.$$

On a en particulier, en posant $\frac{te^{Xt}}{e^t - 1} = F(t, X)$:

$$\sum_{a \in [1,f]'} \frac{\chi(a) t e^{at}}{e^{ft} - 1} = \frac{1}{f} \sum_{a \in [1,f]'} \chi(a) F\left(ft, \frac{a}{f}\right),$$

soit :

$$B_n(\chi) = \frac{1}{f} \sum_{a \in [1,f]'} \chi(a) f^n \mathbb{B}_n\left(\frac{a}{f}\right).$$

(5.3.1) **Remarque.** Nous donnons, pour les nombres de Bernoulli, une définition différente de celles de [L], [B–S], [W], qui tient compte des définitions relatives aux distributions de Stickelberger et qui permet d'éviter une aberration pourtant classique, lorsque χ est le caractère unité modulo 1 : en effet, pour $\chi = \chi_0$ et $f = 1$, on a $[1, f]' = [1, 1]' = \{1\}$ et $\chi_0(1) = 1$; la sommation (5.3) sur $a \in [1, f]'$ devient donc $\frac{te^t}{e^t - 1}$ qui est $\sum_{n \geq 0} B_n \frac{t^n}{n!} =$

$\sum_{n\geq 0} B_n(\chi_0)\frac{t^n}{n!}$ (au sens des nombres de Bernoulli ordinaires comme au sens des nombres de Bernoulli généralisés).
On a en particulier :

$$B_0(\chi_0) = B_0 = 1 \ ; \ B_1(\chi_0) = B_1 = \frac{1}{2} \ ; \ B_2(\chi_0) = B_2 = \frac{1}{6}. \tag{5.3.2}$$

On a alors facilement :

$$\mathbb{B}_n(X) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} B_i X^{n-i}, \text{ pour tout } n \geq 0, \tag{5.3.3}$$

où $\binom{n}{i} = \frac{n!}{i!(n-i)!}$;

en particulier,

$$\mathbb{B}_0(X) = 1, \mathbb{B}_1(X) = X - \frac{1}{2}, \mathbb{B}_2(X) = X^2 - X + \frac{1}{6}. \tag{5.3.4}$$

Pour l'étude des propriétés des nombres et polynomes de Bernoulli, qui découlent de la définition, se reporter à [L], [B–S], [W] (et tenir compte de (5.3.2)); signalons seulement que le lien que nous avons évoqué ci-dessus avec les distributions St est donné (avant la théorie des fonctions L p-adiques) par le résultat suivant :

(5.4) **Proposition.** Pour tout $\chi \in tor(X^{ab})$, on a :

$$\langle \chi, St_{K_\chi} \rangle = -B_1(\chi^{-1}) = \sum_{a \in [1,f]'} \chi^{-1}(a) \left(-\frac{a}{f} + \frac{1}{2} \right).$$

On notera que en remplaçant χ par χ^{-1} et en modifiant le signe on pourrait définir les nombres de Bernoulli d'une façon plus cohérente encore.

Le point de départ de la théorie des fonctions L p-adiques de $\mathbb{Q}$ est le résultat classique suivant d'analyse complexe :

(5.5) **Théorème.** Pour tout $f \geq 1$ et pour tout $c \in (\mathbb{Z}/f\mathbb{Z})^*$, $\zeta_f(c,s)$ admet un prolongement analytique dans $\mathbb{C}$ (avec un pôle en $s = 1$ si $f = 1$) pour lequel

$$\zeta_f(c, 1-n) = -\frac{1}{n} f^{n-1} \mathbb{B}_n \left(\frac{a}{f} \right), \text{ pour tout } n \geq 1,$$

où $a \in [1,f]'$ représente c.

(5.5.1) **Remarque.** On a donc $\zeta_f(c,0) = -\frac{a}{f} + \frac{1}{2}$, $a \in [1,f]'$ représentant c ; en particulier, on a $\zeta_{\mathbb{Q}}(0) = \zeta_1(\mathbb{Z},0) = -\mathbb{B}_1(1) = -\frac{1}{2}$ comme attendu.

(5.5.2) **Corollaire.** Pour tout caractère de Dirichlet χ modulo f, on a

$$L(\chi, 1-n) = -\frac{1}{n} B_n(\chi), \text{ pour tout } n \geq 1.$$

Pour la démonstration de (5.5), on se reportera à la nouvelle démonstration de Stark [St] qui en un sens minimise la partie analyse complexe pour mettre en évidence les aspects qui nous sont utiles ici.

En particulier, la relation (5.2.3) conduit à la relation analogue pour les nombres de Bernoulli généralisés :

$$B_n(\chi) = \prod_{\ell \mid f,\, \ell \nmid f_\chi} \left(1 - \frac{\chi(\ell)}{\ell^{1-n}}\right) . B_n(\chi'), \; n \geq 1. \tag{5.5.3}$$

CHAPITRE V

Fonctions L p-adiques de $\mathbb{Q}$

L'idée de la construction de fonctions L p-adiques, due à Kubota et Leopoldt [K–L], est, comme l'on fait d'une manière générale pour "p-adifier" des fonctions classiques, d'interpoler au mieux les valeurs algébriques remarquables de la fonction étudiée : ces valeurs prises dans $\overline{\mathbb{Q}}$ sont donc dans $\mathbb{C}_p$ puisqu'on a convenu de prendre la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}_p$ et sont donc canoniquement des nombres p-adiques. Ici ces valeurs sont les valeurs prises aux entiers négatifs ; d'après (IV. 5.5.2), ce sont essentiellement des nombres de Bernoulli généralisés. Comme les entiers négatifs constituent un sous-ensemble dense de $\mathbb{Z}_p$, il suffit de voir si la restriction de $L(\chi, s)$ à ces entiers est continue p-adiquement, ou en tout cas si ceci est vrai quitte à effectuer une modification ad'hoc pour y arriver. En fait on parvient directement à une telle interpolation en constatant que des intégrales de caractères continus convenables des distributions de Stickelberger St_S (S contenant p) sont directement liées aux valeurs $L(\chi, 1-n)$, $n \geq 1$, et fournissent donc automatiquement les fonctions L_p cherchées.

Nous ne pouvons citer toutes les références concernant la construction des fonctions L p-adiques de $\mathbb{Q}$; on se reportera pour cela à [B], [Iw], [Ko], [L], [W].

1.— Définition de $L_p(\chi, s)$.

Soit $\chi \in tor(X^{ab})$ un caractère d'ordre fini de G^{ab} vu comme caractère de Dirichlet modulo m multiple de f_χ ; on désigne par S_0 l'ensemble des diviseurs premiers de m distincts de p et on pose :

$$S = S_0 \cup \{p\}. \tag{1.1}$$

On considère les caractères ω et $\langle\ \rangle$ relatifs à p, définis en (IV.2.3) ; on rappelle que ω est de conducteur q et que $\langle\ \rangle$ est un caractère continu d'ordre infini (comme caractère de $\mathbb{Q}_\infty$ on peut dire, par abus de langage, que son ordre et son conducteur sont p^∞). Les caractères χ, ω, $\langle\ \rangle$ et $N = \omega\langle\ \rangle$ sont donc des caractères de $\mathbb{Q}(S)$.

(1.2) **Définition.** Soit St_S la distribution de Stickelberger associée à S (cf. (IV.3.6)), de dénominateur $\delta^\tau = 1 - N\tau.\tau^{-1}$ non nul et non diviseur de 0 dans Λ_S (ce qui d'après (IV.3.6.1) équivaut à prendre $\tau \in G_S$ tel que $\langle\tau\rangle \neq 1$) ; alors on pose :

$$L_p(\chi, s) = \langle \omega\chi^{-1}\ \langle\ \rangle^s,\ St_S \rangle,$$

pour tout $s \in \mathbb{Z}_p$ pour lequel $\langle \omega\chi^{-1}\ \langle\ \rangle^s,\ \delta^\tau \rangle \neq 0$, soit $1 - \chi(\tau)\langle\tau\rangle^{1-s} \neq 0$. Si l'on choisit $\tau \in G_S$ tel que $o(\chi(\tau)) = o(\chi)$ et $\langle\tau\rangle \neq 1$, alors cette condition est réalisée tout le temps sauf pour $s = 1$ si $\chi = \chi_0$.

(1.2.1) **Remarque.** Soit K_χ le sous-corps de $\mathbb{Q}(S)$ fixe par $H = Ker\chi$ et soit $\tau \in G_S$ dont la restriction à K_χ engendre $Gal(K_\chi/\mathbb{Q})$; on a alors $o(\chi(\tau)) = o(\chi) = [K_\chi : \mathbb{Q}]$. Comme $\langle H \rangle \neq \{1\}$ (sinon cela voudrait dire que $\mathbb{Q}_\infty \subseteq K_\chi$) , il suffit de choisir τ modulo H convenablement pour avoir la seconde condition $\langle\tau\rangle \neq 1$.

(1.3) **Conséquences.** (i) Comme $\langle\ \rangle$ est à valeurs dans $1+q\mathbb{Z}_p$, il est clair que $\langle\ \rangle^s$ est un caractère continu pour tout $s \in \mathbb{Z}_p$. On a donc dans (1.2) l'intégrale d'un caractère continu par rapport à une distribution $St_S = \frac{\nu_S^\tau}{\delta^\tau}$, et donc on a :

$$L_p(\chi, s) = (1-\chi(\tau)\langle\tau\rangle^{1-s})^{-1}\ \langle\omega\chi^{-1}\langle\ \rangle^s,\ \nu_S^\tau\rangle\ , \tag{1.3.1}$$

pour tout $s \in \mathbb{Z}_p$, $s \neq 1$ si $\chi = \chi_0$ (sous réserve du choix (1.2.1)).

(ii) D'après (IV.4.8), et compte-tenu du fait que $\langle\ \rangle$ est un caractère pair et ω un caractère impair, on a $L_p(\chi, s) = 0$, pour tout $s \in \mathbb{Z}_p$, dès que χ est impair. On suppose donc désormais χ pair.

(iii) Comme d'après (IV.4.8) il existe une distribution St_S^+, de numérateur défini modulo $(1+\sigma_{-1,S})\Lambda_S$ et de dénominateur δ^τ, telle que

$$St_S = (1-\sigma_{-1,S})St_S^+\ ,$$

on peut considérer que la fonction $L_p(\chi, s)$ n'est pas "primitive" pour la place à l'infini, et que la bonne fonction à considérer (notamment dans le cas $p=2$) est la fonction

$$\frac{1}{2}\ L_p(\chi, s) = \langle\omega\chi^{-1}\langle\ \rangle^s,\ St_S^+\rangle \tag{1.3.2}$$

(intégrale qui ne dépend pas du choix de St_S^+ dès que χ est pair).

(iv) Prenons τ de la forme σ_c, $(c, S) = 1$, de telle sorte que, sauf dans le cas $\chi = \chi_0$ et $s = 1$, on ait $1-\chi(\tau)\langle\tau\rangle^{1-s} = 1-\chi(c)\langle c\rangle^{1-s} \neq 0$ (ceci est possible en vertu de (IV.1.3.2) (i)). Fixons ensuite $St_S^+ = \frac{\nu_S^{\tau+}}{\delta^\tau}$, $\nu_S^{\tau+} \in \Lambda_S$ (définie modulo $(1+\sigma_{-1,S})\Lambda_S$), et posons pour simplifier :

$$\nu_S^{\tau+} = \nu_S^+,\ \delta^\tau = \delta\ .$$

Soit alors ν_F^+ la composante de ν_S^+ sur $\mathbb{Z}_p[G_F]$, $F \in \mathcal{F}_S'$ (cf. (IV.3.1)) de conducteur f : on rappelle (cf. (IV.3.6)) que l'on a

$$\nu_F = \delta_F\rho_F = \sum_{a\in[1,f]'} R_a^c\sigma_{a,F}^{-1},\ \text{où}\ R_a^c = r_a^c + \frac{1-c}{2},$$

où $r_a^c = \frac{1}{f}\left([\frac{a}{c}]_f\ c - a\right)$, $[\frac{a}{c}]_f$ étant l'unique représentant entier modulo f de $\frac{a}{c}$ dans l'intervalle $[1, f]$.

On a $r_{f-a}^c = \frac{1}{f}\left([\frac{f-a}{c}]_f\ c - (f-a)\right)$; mais comme $[\frac{f-a}{c}]_f \equiv -\frac{a}{c} \bmod f$ et $f > 1$, on a $[\frac{f-a}{c}]_f = f - [\frac{a}{c}]_f$, et $r_{f-a}^c = \frac{1}{f}\left(fc - [\frac{a}{c}]_f\ c - f + a\right) = c - 1 - r_a^c$; par conséquent, on a

$$R_{f-a}^c = -R_a^c \text{ pour tout } a \in [1, f]'. \tag{1.3.3}$$

D'où facilement :

$$\nu_F = \sum_{a\in[1,f]'} R_a^c\sigma_{a,F}^{-1} = (1-\sigma_{-1,F}) \sum_{a\in[1,\frac{f}{2}]'} R_a^c\sigma_{a,F}^{-1}, \tag{1.3.4}$$

et on en déduit que la composante ν_F^+ de ν_S^+ vérifie la congruence :

$$\nu_F^+ \equiv \sum_{a\in[1,\frac{f}{2}]'} R_a^c \sigma_{a,F}^{-1} \mod (1+\sigma_{-1,F})\mathbb{Z}_p[G_F]. \tag{1.3.5}$$

On notera qu'il n'y a pas nécessairement égalité ; cependant pour le calcul des intégrales d'un caractère pair, on peut remplacer tout prolongement de ν_F^+ dans $\mathbb{Z}_p[G_S]$ par n'importe quel prolongement du second membre de (1.3.5).

En utilisant (II.5.3.1), on en déduit que (pour $s \neq 1$ si $\chi = \chi_0$) l'on a, selon la forme utilisée :

$$L_p(\chi,s) = (1-\chi(c)\langle c\rangle^{1-s})^{-1} \lim_{\substack{f\to 0\\ f\in\mathbb{N}_S'}} \langle \omega\chi^{-1}\langle\ \rangle^s, \nu_F'\rangle,$$

$$\frac{1}{2}\, L_p(\chi,s) = (1-\chi(c)\langle c\rangle^{1-s})^{-1} \lim_{\substack{f\to 0\\ f\in\mathbb{N}_S'}} \langle \omega\chi^{-1}\langle\ \rangle^s, \nu_F^{+\prime}\rangle,$$

où ν_F' et $\nu_F^{+\prime} \in \mathbb{Z}_p[G_S]$ sont des prolongements arbitraires de ν_F et ν_F^+ dans $\mathbb{Z}_p[G_S]$; on notera que $f \to 0$ p-adiquement, $f \in \mathbb{N}_S'$, traduit la condition $Gal(\mathbb{Q}(S)/F) \to \{1\}$ du passage à la limite sur $F \in \mathcal{F}_S'$ (cf. (IV.3.1)).

Il reste à préciser ν_F' et $\nu_F^{+\prime}$ sachant (cf. (1.3.4), (1.3.5)) que $\nu_F = \sum_{a\in[1,f]'} R_a^c\sigma_{a,F}^{-1}$ et $\nu_F^+ \equiv \sum_{a\in[1,\frac{f}{2}]'} R_a^c\sigma_{a,F}^{-1} \mod (1+\sigma_{-1,F})\mathbb{Z}_p[G_F]$; il est naturel de prolonger ν_F en

$$\nu_F' = \sum_{a\in[1,f]'} R_a^c\sigma_a^{-1} \tag{1.3.6}$$

qui n'est plus un élément de $(1-\sigma_{-1})\mathbb{Z}_p[G_S]$ (en effet, pour $a \in [1,\frac{f}{2}]'$, on a $R_{f-a}^c\sigma_{f-a}^{-1} = -R_a^c\sigma_{-1}\sigma_a^{-1}\sigma_u^{-1}$, où $u = 1-a^{-1}f$) ; on est donc amené à considérer :

$$\nu_F^{+\prime\prime} = \sum_{a\in[1,\frac{f}{2}]'} R_a^c\sigma_a^{-1} \tag{1.3.7}$$

et donc

$$\nu_F'' = (1-\sigma_{-1})\nu_F^{+\prime\prime} \in (1-\sigma_{-1})\mathbb{Z}_p[G_S]\ .$$

On obtient ainsi 2 prolongements distincts de ν_F.

En ce qui concerne ν_F^+, on a d'après (1.3.5) :

$$\nu_F^+ = \sum_{a\in[1,\frac{f}{2}]'} R_a^c\sigma_{a,F}^{-1} + (1+\sigma_{-1,F})\alpha_F,\ \alpha_F \in \mathbb{Z}_p[G_F]$$

qui admet un prolongement de la forme

$$\nu_F^{+\prime} = \sum_{a\in[1,\frac{f}{2}]'} R_a^c\sigma_a^{-1} + (1+\sigma_{-1})\alpha_F^{'},$$

pour $\alpha_F^{'}$ prolongeant α_F. On a donc :

$$\nu_F^{+\prime} \equiv \nu_F^{+\prime\prime} = \sum_{a\in[1,\frac{f}{2}]'} R_a^c\sigma_a^{-1} \mod (1+\sigma_{-1})\mathbb{Z}_p[G_S]. \tag{1.3.8}$$

Finalement on utilisera les 2 expressions suivantes :

$$\begin{aligned} L_p(\chi,s) &= \lim_{f\to 0}\,(1-\chi(c)\langle c\rangle^{1-s})^{-1}\langle\omega\chi^{-1}\langle\ \rangle^s,\ \nu_F^{'}\rangle \\ &= (1-\chi(c)\langle c\rangle^{1-s})^{-1}\lim_{f\to 0}\sum_{a\in[1,f]'} R_a^c\omega^{-1}\chi(a)\langle a\rangle^{-s}, \end{aligned} \tag{1.3.9}$$

$$\begin{aligned} \frac{1}{2}\,L_p(\chi,s) &= \lim_{f\to 0}\,(1-\chi(c)\langle c\rangle^{1-s})^{-1}\langle\omega\chi^{-1}\langle\ \rangle^s,\ \nu_F^{+\prime\prime}\rangle \\ &= (1-\chi(c)\langle c\rangle^{1-s})^{-1}\lim_{f\to 0}\sum_{a\in[1,\frac{f}{2}]'} R_a^c\omega^{-1}\chi(a)\langle a\rangle^{-s}. \end{aligned} \tag{1.3.10}$$

(1.3.11) **Remarque.** Dans toutes ces expressions, on peut toujours supposer que $F = \mathbb{Q}(f)$, $f\in\mathbb{N}_S^{'}$, $f\to 0$ (p-adiquement).

On a le résultat fondamental suivant, justifiant a posteriori les définitions précédentes :

(1.4) **Théorème.** Pour tout caractère $\chi\in tor(X^{ab})$ et pour tout $n\geq 1$, on a (où les caractères écrits sont primitifs) :

$$L_p(\chi,1-n) = -(1-\chi\omega^{-n}(p)p^{n-1})\frac{B_n(\chi\omega^{-n})}{n}.$$

On en déduit l'expression suivante qui exprime de quelle façon (autre que l'égalité $L_p(\chi,1-n)=L(\chi,1-n)$) la fonction L_p interpole continuement les valeurs aux entiers négatifs de $L(\chi,s)$:

(1.4.1) **Corollaire.** On a en particulier (cf. (IV.5.5, 5.5.2)) :

$$L_p(\chi,1-n) = (1-\chi\omega^{-n}(p)p^{n-1})L(\chi\omega^{-n},1-n),\ n\geq 1.$$

(1.4.2) **Remarques.** (i) Dans (1.4) et (1.4.1), les caractères χ, $\chi\omega^{-n}$ sont vus comme caractères primitifs ; en particulier, si χ est de conducteur f_χ, et si $\chi\omega^{-n}\neq\chi$ (i.e. $n\not\equiv 0 \mod \varphi(q)$), alors $\chi\omega^{-n}$ a pour conducteur :

$$qf_\chi \text{ si } f_\chi\not\equiv 0 \mod p,$$

$$f_\chi \quad \text{si } f_\chi \equiv 0 \mod p,$$

sauf dans le cas particulier où $\chi = \omega^n\psi$, ψ de conducteur f_ψ étranger à p, auquel cas $\chi\omega^{-n} = \psi$ est de conducteur $f_\psi = q^{-1}f_\chi$. Cependant dans tous les cas, la formule de (1.4) peut s'écrire de façon imprimitive :

$$(1.4)' \qquad L_p(\chi, 1-n) = -\frac{B_n(\chi\omega^{-n})}{n}, n \geq 1,$$

en considérant $\chi\omega^{-n}$ comme caractère de Dirichlet modulo f, où $f = f_\chi$ ou qf_χ selon que p divise f_χ ou non, et même plus généralement modulo $f \in \mathbb{N}'_S$ en vertu de (IV.5.5.3).

(ii) Si χ est un caractère de Dirichlet modulo f non nécessairement primitif, alors l'expression (IV.4.6) montre que l'on a :

$$L_p(\chi, s) = L_p(\chi', s) \prod_\ell \left(1 - \frac{\chi(\ell)}{\ell}\,\langle\ell\rangle^{1-s}\right),$$

où χ' désigne le caractère primitif déduit de χ, le produit portant sur les premiers ℓ, $\ell \neq p$, $\ell | f$ et $\ell \nmid f_\chi$. Ceci est cohérent avec les différentes propriétés eulériennes puisque pour $s = 1-n$, $n \geq 1$, on a $1 - \frac{\chi(\ell)}{\ell}\,\langle\ell\rangle^{1-s} = 1 - \chi\omega^{-n}(\ell)\,\ell^{n-1}$.

(iii) On peut considérer que lorsque $f_\chi = f$ est étranger à p, $L_p(\chi, s)$ n'est pas vraiment une fonction L_p primitive ; en particulier, lorsque $\chi\omega^{-1}(p) = 1$ (i.e. p totalement décomposé dans $K_{\omega\chi^{-1}}$), on a, d'après (1.4.1),

$$L_p(\chi, 0) = (1 - \chi\omega^{-1}(p))\, L(\chi\omega^{-1}, 0) = 0$$

par annulation du facteur eulérien ; ce zéro particulier s'appelle le zéro trivial de $L_p(\chi, s)$ et on a pu démontrer qu'il était simple (cf. [F-G]). Ces inconvénients d'imprimitivité des fonctions L_p viennent du fait que l'on est obligé d'utiliser le plus petit groupe G_S sur lequel les caractères utilisés soient définis ; or les caractères ω et $\langle\ \rangle$ supposent que $p \in S$.

(iv) L'égalité $L_p(\chi, 1-n) = L(\chi, 1-n)$ n'a lieu que sur les entiers négatifs $1-n$ tels que $n \equiv 0 \mod \varphi(q)$ et l'écriture est primitive uniquement si $f_\chi \equiv 0 \mod p$.

démonstration de (1.4).

Considérons

$$(1.4.3) \qquad \begin{aligned} A_f &= \sum_{a \in [1,f]'} -\frac{a}{f}\,\omega^{-1}\chi(a)\langle a\rangle^{-s} \\ &= -\frac{1}{f}\sum_{a \in [1,f]'} \chi(a)\langle a\rangle^{1-s}, \end{aligned}$$

et calculons une valeur approchée de

$$B_f^c = (1 - \chi(c)\langle c\rangle^{1-s})\, A_f,\ (c, f) = 1,\ \langle c\rangle \neq 1.$$

Il vient :

$$B_f^c = \sum_{b\in[1,f]'} \Big(-\frac{1}{f}\langle b\rangle^{1-s}\chi(b) + \frac{1}{f}\langle bc\rangle^{1-s}\chi(bc)\Big);$$

posons comme d'habitude $bc = r_a^c f + a$, $a \in [1,f]'$, et écrivons

$$\langle a + r_a^c f\rangle^{1-s} = \langle a\rangle^{1-s}(1 + a^{-1}r_a^c f)^{1-s};$$

d'après le lemme (1.4.6) prouvé plus loin, on a

$$(1 + a^{-1}r_a^c f)^{1-s} \equiv 1 + (1-s)a^{-1}\, r_a^c f \mod \frac{1}{2}\, s(1-s)f^2.$$

Il vient alors

$$\begin{aligned} B_f^c &\equiv \sum_{a\in[1,f]'} \langle a\rangle^{1-s}\chi(a)\Big(-\frac{1}{f} + \frac{1}{f} + (1-s)a^{-1}r_a^c\Big) \\ &\equiv (1-s)\sum_{a\in[1,f]'} \langle a\rangle^{1-s}a^{-1}r_a^c\chi(a) \\ &\equiv (1-s)\sum_{a\in[1,f]'} \omega^{-1}\chi(a)\langle a\rangle^{-s}r_a^c \bmod \frac{1}{2}\, s(1-s)f; \end{aligned}$$

comme d'après (1.4.7) (voir également plus loin) on a

$$\lim_{f\to 0} \sum_{a\in[1,f]'} \omega^{-1}\chi(a)\langle a\rangle^{-s} = 0,$$

on déduit que B_f^c a même limite, lorsque $f \to 0$, $f \in \mathbb{N}_S'$, que

$$(1-s)\sum_{a\in[1,f]'} \omega^{-1}\chi(a)\langle a\rangle^{-s}R_a^c,$$

puisque $R_a^c = r_a^c + \frac{1-c}{2}$. En rapprochant ceci de l'expression (1.3.9) de $L_p(\chi,s)$, on obtient (pour $s \neq 1$) :

$$\begin{aligned} L_p(\chi,s) &= \frac{1}{1-s}\,(1-\chi(c)\langle c\rangle^{1-s})^{-1}\lim_{f\to 0}\, B_f^c \\ &= \frac{1}{1-s}\lim_{f\to 0}\, A_f, \text{ par définition de } B_f^c, \end{aligned}$$

d'où, d'après (1.4.3) :

$$L_p(\chi,s) = \frac{1}{1-s}\,\lim_{f\to 0}\,\frac{-1}{f}\sum_{a\in[1,f]'}\chi(a)\langle a\rangle^{1-s},\ s\neq 1. \tag{1.4.4}$$

Ayant obtenu cette expression, nous donnons en (1.5) une estimation précise de l'approximation

$$L_p(\chi,s)-\frac{1}{1-s}\Big(-\frac{1}{f}\sum_{a\in[1,f]'}\chi(a)\langle a\rangle^{1-s}\Big)$$

traduite par la limite ci-dessus.

Remarque. On constate à ce niveau que l'intégrale $\langle\omega\chi^{-1}\langle\ \rangle^s, St_S\rangle$ définissant $L_p(\chi,s)$ ne saurait être une limite de la forme suivante, pour le prolongement évident ρ_F' de ρ_F dans $\mathbb{Q}[G_S]$:

$$\begin{aligned}\lim_{f\to 0}\langle\omega\chi^{-1}\langle\ \rangle^s,\ \rho_F'\rangle &= \lim_{f\to 0}\sum_{a\in[1,f]'}\Big(\frac{-a}{f}+\frac{1}{2}\Big)\omega^{-1}\chi(a)\langle a\rangle^{-s}\\ &= \lim_{f\to 0}\frac{-1}{f}\sum_{a\in[1,f]'}\chi(a)\langle a\rangle^{1-s}\ \text{ d'après (1.4.7)}\end{aligned}$$

(qui est donc $(1-s)L_p(\chi,s)$ au lieu de $L_p(\chi,s)$, en vertu de (1.4.4)) ; ceci proviendrait du raisonnement faux suivant sur l'utilisation des distributions : on a

$$\begin{aligned}L_p(\chi,s) &= \langle\omega\chi^{-1}\langle\ \rangle^s,\delta\rangle^{-1}\ \langle\omega\chi^{-1}\langle\ \rangle^s,\nu_S\rangle\\ &= \langle\omega\chi^{-1}\langle\ \rangle^s,\delta\rangle^{-1}\ \lim_{f\to 0}\langle\omega\chi^{-1}\langle\ \rangle^s,\nu_F'\rangle\\ &= \lim_{f\to 0}\frac{\langle\omega\chi^{-1}\langle\ \rangle^s,\nu_F'\rangle}{\langle\omega\chi^{-1}\langle\ \rangle^s,\delta\rangle}\\ &= \lim_{f\to 0}\langle\omega\chi^{-1}\langle\ \rangle^s,\frac{\nu_F'}{\delta}\rangle\ \text{(ce qui est exact)}\\ &= \lim_{f\to 0}\langle\omega\chi^{-1}\langle\ \rangle^s,\rho_F'\rangle\ \text{(ce qui est faux)}\end{aligned}$$

qui est dû tout simplement au fait que $\delta\rho_F'$ est non seulement distinct de ν_F' mais n'est pas un prolongement de ν_F : il en diffère d'un élément de l'idéal d'augmentation de $\mathbb{Q}_p[G_S]$ (et non de $\mathbb{Z}_p[G_S]$) dont les dénominateurs proviennent des $\frac{1}{f}$.

Revenons à (1.4.4) ; pour $s=1-n$, $n\geq 1$, on obtient

$$\begin{aligned}L_p(\chi,1-n) &= -\frac{1}{n}\lim_{f\to 0}\frac{1}{f}\sum_{a\in[1,f]'}\chi(a)\langle a\rangle^n\\ &= -\frac{1}{n}\lim_{f\to 0}\frac{1}{f}\sum_{a\in[1,f]'}\chi\omega^{-n}(a)a^n.\end{aligned}$$

On a par ailleurs, pour tout $f\in\mathbb{N}_S'$ (cf. (IV.5.3), (ii)) :

$$B_n(\chi\omega^{-n})=\frac{1}{f}\sum_{a\in[1,f]'}\chi\omega^{-n}(a)f^n\mathbb{B}_n\Big(\frac{a}{f}\Big)$$

avec

$$f^n \mathbb{B}_n(\frac{a}{f}) = f^n \sum_{i=0}^{n} (-1)^i \binom{n}{i} B_i (\frac{a}{f})^{n-i}$$
$$= \sum_{i=0}^{n} (-1)^i \binom{n}{i} B_i a^{n-i} f^i \ ;$$

en écrivant que

$$B_n(\chi\omega^{-n}) = \lim_{\substack{f \to 0 \\ f \in \mathbb{N}'_S}} \frac{1}{f} \sum_{a \in [1,f]'} \chi\omega^{-n}(a) \sum_{i=0}^{n} (-1)^i \binom{n}{i} B_i a^{n-i} f^i \ ,$$

on voit que cette limite est celle de

$$\frac{1}{f} \sum_{a \in [1,f]'} \chi\omega^{-n}(a)(a^n - f\frac{n}{2}a^{n-1}) \ ,$$

et donc celle de

$$\frac{1}{f} \sum_{a \in [1,f]'} \chi\omega^{-n}(a) a^n$$

en utilisant à nouveau (1.4.7). D'où le théorème (1.4).

Démontrons maintenant les lemmes que nous avons utilisés, sous la forme optimale qui nous sera nécessaire ultérieurement ; pour cela nous avons besoin de la définition suivante :

(1.4.5) **Définition**. Soit $\mathcal{O}_p$ l'anneau des entiers de $\mathbb{C}_p$ et soit $\mathcal{M}_p$ son idéal maximal ; on définit la $\mathcal{O}_p$-algèbre $\mathcal{A}$ des fonctions $g : \mathbb{Z}_p \to \mathcal{O}_p$ qui admettent un développement en "série d'Iwasawa" de la forme

$$g(s) = \sum_{i \geq 0} a_i s^i, \ a_i \in \mathcal{O}_p \ \text{ et } \lim_i a_i = 0 \ .$$

On vérifie facilement les points suivants (outre le fait qu'il s'agit bien d'une $\mathcal{O}_p$-algèbre) :

(i) le développement est unique ;

(ii) pour tout $u \in \mathcal{O}_p^*$, $v \in \mathcal{O}_p$, g est développable en série unique de la forme

$$g(s) = \sum_{i \geq 0} a'_i (us + v)^i, \ a'_i \in \mathcal{O}_p \ \text{ et } \lim_i a'_i = 0 \ ;$$

(iii) on a $\mathcal{A}^* = \mathcal{O}_p^* + \mathcal{M}_p \mathcal{A}$;

(iv) les éléments de $\mathcal{A}$ sont des fonctions continues indéfiniment dérivables ;

(v) pour tout a étranger à p, $\langle a \rangle^s \in \mathcal{A}$.

(1.4.6) **Lemme.** Soit f un multiple de q, soit $u \in \mathbb{Z}_p$; alors on a, pour $s \in \mathbb{Z}_p$:

$$(1+uf)^{1-s} \equiv 1 + (1-s)uf - \frac{1}{2}\, s(1-s)u^2f^2 \mod 2s(1-s)(1+s)f^2\mathcal{A}\,.$$

Ecrivons le développement convergent

$$(1+uf)^{1-s} = 1 + (1-s)uf + \frac{1}{2}(1-s)(-s)u^2f^2$$

$$+\sum_{n\geq 3} \frac{(1-s)(1-s-1)\ldots(1-s-(n-1))}{n!}u^nf^n$$

$$= 1 + (1-s)uf - \frac{1}{2}\, s(1-s)u^2f^2$$

$$+2s(1-s)(1+s)f^2 \sum_{n\geq 3} (1-s-3)\ldots(1-s-(n-1))\frac{u^nf^{n-2}}{2.n!}\,.$$

On a $v(n!) = \frac{n-\sigma(n)}{p-1}$, où $\sigma(n) = \sum_{i\geq 0}\ a_i$, si $n = \sum_{i\geq 0}\ a_ip^i$ est l'écriture en base p de n ; par conséquent, pour un calcul modulo $2s(1-s)(1+s)f^2\mathcal{A}$, il suffit de négliger les termes d'indices $n \geq 3$ tels que (selon que $p \neq 2$ ou $p = 2$) :

$$(n-2)v(f) - \frac{n-\sigma(n)}{p-1}\ \geq 0 \quad (\text{resp. } \geq 1)\ ;$$

il suffit que n soit tel que

$$n - 2 - \frac{n-\sigma(n)}{p-1}\ \geq 0 \quad (\text{resp. } 2(n-2) - (n-\sigma(n)) \geq 1)\ .$$

Pour $p \neq 2$ il vient $n(p-2) - 2(p-1) + \sigma(n) \geq 0$, et pour $n \geq 3$, on a $n(p-2) - 2(p-1) + \sigma(n) \geq p - 4 + \sigma(n) \geq 0$ puisque $\sigma(n) \geq 1$. Pour $p = 2$, il vient $n - 5 + \sigma(n) \geq 0$; pour $n = 3$, on a $\sigma(3) = 2$ et $n - 5 + \sigma(n) = 0$; pour $n \geq 4$, l'inégalité est toujours vérifiée puisque $\sigma(n) \geq 1$.

D'où le lemme puisque pour tout $n \geq 3$, $(1-s-3)\ldots(1-s-(n-1))\frac{u^nf^{n-2}}{2.n!}$ est un polynome en s à coefficients dans $\mathbb{Z}_p$ et que $\frac{f^{n-2}}{2.n!} \to 0$ si $n \to \infty$.

(1.4.7) **Lemme.** Soit ψ un caractère continu de G_S, S contenant p, et soit $f \in \mathbb{N}'_S$ tendant p-adiquement vers 0 ; alors on a

$$\lim_{f\to 0} \sum_{a\in[1,f]'} \psi(\sigma_a) = 0\ .$$

Si $\psi = \chi_0$, la somme ci-dessus est égale à $\varphi(f)$, où φ est l'indicateur d'Euler ; d'où le résultat dans ce cas.

Supposons $\psi \neq \chi_0$ et soit e entier étranger à S tel que $\psi(\sigma_e) \neq 1$ (ceci est possible en vertu de (IV.1.3.2), (i), compte-tenu de la continuité de ψ) ; on a alors

$$(1-\psi(\sigma_e)) \sum_{a\in[1,f]'} \psi(\sigma_a) = \sum_{b\in[1,f]'} \psi(\sigma_b) - \psi(\sigma_{eb}) ,$$

et en posant $ab = a + r_a^c f$, $a \in [1,f]'$, l'expression ci-dessus devient

$$\sum_{a\in[1,f]'} \psi(\sigma_a)(1-\psi(\sigma_u)),\ u = 1 + a^{-1} r_a^e f ;$$

or si $f \to 0$ dans $\mathbb{N}_S'$, on a, uniformément en u, $\sigma_u \to 1$ et $\psi(\sigma_u) \to 1$. D'où le lemme.

Nous pouvons maintenant donner une première congruence permettant d'approcher $\frac{1}{2} L_p(\chi, s)$ (pour une approche numérique différente, voir §6) :

(1.5) **Théorème.** Soit $\chi \in tor(X^{ab})$, χ pair, et soit $f \in \mathbb{N}_S'$, où S est l'ensemble des diviseurs premiers de pf_χ. On a, pour tout $s \in \mathbb{Z}_p$, $s \neq 1$ (pour $s = 1$, voir (1.7)) :

$$(1-s)\frac{1}{2} L_p(\chi, s) \equiv -\frac{1}{2f} \sum_{a\in[1,f]'} \chi(a)\langle a\rangle^{1-s} + N(s) \bmod M(s)\mathcal{A} ,$$

où $N(s)$ et $M(s)$ sont ainsi définis :

(i) $\chi \neq \omega^2$. Alors $N(s) = 0$ et

(α) $M(s) = s(1-s)(1+s)f$ si $o(\chi)$ n'est pas une puissance de p ;

(β) $M(s) = s(1-s)(1+s)\frac{f}{\pi}$ si $o(\chi) = p^r$, $r \geq 1$, où π est une uniformisante de $\mathbb{Q}_p(\chi)$;

(γ) $M(s) = s(1+s)\frac{f}{p}$ si $\chi = \chi_0$.

(ii) $\chi = \omega^2$; on a :

(α) $N(s) = -\frac{1}{12} f\varphi(f)s(1-s)$, $M(s) = s(1-s)(1+s)f$, pour tout $p \geq 5$;

(β) $N(s) = -\frac{1}{6} f\varphi(f)s$, $M(s) = \frac{1}{3} s(1+s)f$ si $p = 3$;

(γ) $N(s) = -\frac{1}{6} f\varphi(f)s$, $M(s) = \frac{1}{4} s(1+s)f$ si $p = 2$.

démonstration

Considérons la mesure $\nu_S^+ = \nu_S^{\tau+}$ introduite en (IV.4.8), prenons τ de la forme σ_c (cf. (1.3), (iv)) et appliquons (1.3.10), pour f fixé et $F = \mathbb{Q}(f)$, à $F' = \mathbb{Q}(f')$, $f, f' \in \mathbb{N}_S'$, $f \mid f'$; il vient, en posant $u_c = 1 - \chi(c)\langle c\rangle^{1-s}$:

$$\frac{1}{2} L_p(\chi, s) - u_c^{-1}\langle\omega\chi^{-1}\langle\ \rangle^s, \nu_F^{+\prime\prime}\rangle =$$

$$\lim_{f'\to 0} u_c^{-1}\langle\omega\chi^{-1}\langle\ \rangle^s, \nu_{F'}^{+\prime\prime}\rangle - u_c^{-1}\langle\omega\chi^{-1}\langle\ \rangle^s, \nu_F^{+\prime\prime}\rangle$$

$$= u_c^{-1} \lim_{f' \to 0} \langle \omega\chi^{-1}\langle\ \rangle^s, \nu_{F'}^{+\prime} - \nu_F^{+\prime} \rangle \ \text{(cf.(1.3.8))} ;$$

puisque l'on a $F \subseteq F'$ et que ν_S^+ est une mesure, on a

$$\begin{aligned}(\nu_{F'}^{+\prime} - \nu_F^{+\prime})_F &= (\nu_{F'}^+)_F - (\nu_F^{+\prime})_F \\ &= \nu_{F',F}^+ - \nu_F^+ = 0,\end{aligned}$$

et par conséquent, $\nu_{F'}^{+\prime} - \nu_F^{+\prime}$ appartient à l'idéal d'augmentation de $\mathbb{Z}_p[Gal(\mathbb{Q}(S)/F)]$ i.e. l'idéal engendré par les $1-\sigma$, σ fixant $F = \mathbb{Q}(f)$; comme $\{\sigma_h,\ h = 1+\lambda f,\ \lambda \in \mathbb{Z}, (h,S) = 1\}$ est dense dans $Gal(\mathbb{Q}(S)/F)$ et que $\langle \omega\chi^{-1}\langle\ \rangle^s, 1-\sigma_h\rangle = 1-(1+\lambda f)^s \equiv 0 \mod sf\mathcal{A}$ (cf. (1.4.6)), on en déduit que $\langle \omega\chi^{-1}\langle\ \rangle^s, 1-\sigma\rangle \in sf\mathcal{A}$ et que

$$\frac{1}{2} L_p(\chi, s) - u_c^{-1}\langle \omega\chi^{-1}\langle\ \rangle^s, \nu_F^{+\prime\prime}\rangle \equiv 0 \mod u_c^{-1} sf\mathcal{A} ;$$

ce que nous écrirons sous la forme :

$$(1.5.1) \qquad (1-s)\frac{1}{2} L_p(\chi, s) \equiv u_c^{-1}(1-s)\langle \omega\chi^{-1}\langle\ \rangle^s, \nu_F^{+\prime\prime}\rangle \mod u_c^{-1} s(1-s) f\mathcal{A} .$$

Calculons alors

$$u_c^{-1}(1-s)\langle \omega\chi^{-1}\langle\ \rangle^s, \nu_F^{+\prime\prime}\rangle \mod u_c^{-1} s(1-s) f\mathcal{A} ,$$

ce qui donne bien $(1-s)\frac{1}{2} L_p(\chi, s)$ selon ce module, lequel est optimal lorsque $v(u_c)$ est minimale. On a $u_c = 1 - \chi(c)\langle c\rangle^{1-s} \equiv 1 - \chi(c) \mod q\mathcal{A}$; donc si $o(\chi)$ n'est pas une puissance de p et si l'on choisit c tel que $\chi(c)$ soit une racine de l'unité d'ordre égal à $o(\chi)$, on a $u_c \in \mathcal{A}^*$; si $o(\chi) = p^r$, $r \geq 1$, pour un choix analogue de c, on a $u_c \equiv \pi \mod \pi^2\mathcal{A}$, où $\pi = 1 - \chi(c)$ est une uniformisante de $\mathbb{Q}(\chi)$, et on a $q \equiv 0 \mod \pi^2$; enfin, si $\chi = \chi_0$, $u_c = 1 - \langle c\rangle^{1-s} \in q(1-s)\mathcal{A}^*$ dès que $\langle c\rangle \in 1 + q\mathbb{Z}_p^*$.

Définissons

$$(1.5.2) \qquad A_f' = \sum_{a \in [1,f]'} \left(\frac{-a}{f} + \frac{1-s}{2}\right) \omega^{-1}\chi(a)\langle a\rangle^{-s},\ B_f'^c = u_c A_f' ,$$

que l'on cherche à calculer modulo $2s(1-s)f\mathcal{A}$. On a

$$\begin{aligned} B_f'^c &= (1-\chi(c)\langle c\rangle^{1-s}) \sum_{b\in[1,f]'} \frac{-b}{f}\, \omega^{-1}\chi(b)\langle b\rangle^{-s} \\ &\qquad + \frac{1-s}{2}\,(1-\chi(c)\langle c\rangle^{1-s}) \sum_{b\in[1,f]'} \omega^{-1}\chi(b)\langle b\rangle^{-s} \\ &= (1-\chi(c)\langle c\rangle^{1-s}) \sum_{b\in[1,f]'} -\frac{1}{f}\,\chi(b)\langle b\rangle^{1-s} \\ &\qquad + \frac{1-s}{2}\,(1-\chi(c)\langle c\rangle^{1-s}) \sum_{b\in[1,f]'} \chi(b)\langle b\rangle^{1-s} b^{-1}; \end{aligned}$$

en écrivant comme d'habitude $\langle bc\rangle^{1-s} = \langle a\rangle^{1-s}(1+a^{-1}r_af)^{1-s}$, $a \in [1,f]'$, $r_a = r_a^c$, et en utilisant le développement (1.4.6), il vient :

$$B_f'^c \equiv (1-s)\sum_{a\in[1,f]'} \chi(a)\langle a\rangle^{1-s}a^{-1}(r_a - \frac{1}{2}\,sa^{-1}r_a^2f) + \frac{1-s}{2}\sum_{a\in[1,f]'} \chi(a)\langle a\rangle^{1-s}a^{-1}(1-c(1+a^{-1}r_af)^{-s}) \mod 2s(1-s)f\mathcal{A}.$$

Or $1-c(1+a^{-1}r_af)^{-s} \equiv 1-c(1-sa^{-1}r_af+\frac{1}{2}\,(1+s)sa^{-2}r_a^2f^2) \equiv 1-c+sca^{-1}r_af - \frac{1}{2}\,(1+s)sca^{-2}r_a^2f^2 \mod 2sf^2\mathcal{A}$. Comme les calculs sont conduits modulo $2s(1-s)f\mathcal{A}$ et que $s(1-s)f^2 \equiv 0 \mod 2s(1-s)f$, il vient

$$\begin{aligned} B_f'^c \equiv{}& (1-s)\sum_{a\in[1,f]'} \chi(a)\langle a\rangle^{1-s}a^{-1}(r_a - \frac{1}{2}sa^{-1}r_a^2f) \\ &+ (1-s)\frac{1-c}{2}\sum_{a\in[1,f]'} \chi(a)\langle a\rangle^{1-s}a^{-1} \\ &+ s\,\frac{1-s}{2}\,cf\sum_{a\in[1,f]'} \chi(a)\langle a\rangle^{1-s}a^{-2}r_a \\ &- \frac{1}{4}\,s(1-s)(1+s)cf^2\sum_{a\in[1,f]'} \chi(a)\langle a\rangle^{1-s}a^{-3}r_a^2 \end{aligned}$$

$\mod 2s(1-s)f\mathcal{A}$, ce qui, en regroupant convenablement s'écrit

$$\begin{aligned} B_f'^c &\equiv (1-s)\sum_{a\in[1,f]'} \omega^{-1}\chi(a)\langle a\rangle^{-s}(r_a + \frac{1-c}{2}) \\ &\quad + \frac{1}{2}\,s(1-s)f\sum_{a\in[1,f]'} \chi(a)\langle a\rangle^{1-s}a^{-2}(-r_a^2 + cr_a - \frac{1}{2}\,(1+s)fca^{-1}r_a^2) \\ &\equiv (1-s)\langle\omega\chi^{-1}\langle\ \rangle^s, \nu_F'\rangle + \frac{1}{2}\,s(1-s)fY \mod 2s(1-s)f\mathcal{A}, \end{aligned}$$

en appelant Y la seconde sommation ci-dessus.

Pour $p \neq 2$, on obtient

$$B_f'^c = u_cA_f'^c \equiv (1-s)\langle\omega\chi^{-1}\langle\ \rangle^s, \nu_F'\rangle \mod s(1-s)f\mathcal{A}. \tag{1.5.3}$$

Supposons maintenant $p=2$ et calculons Y modulo $4\mathcal{A}$ (on a donc $f \equiv 0\ (4)$) :

$$Y \equiv \sum_{a\in[1,f]'} \chi(a)(-r_a^2 + cr_a - (1+s)\frac{f}{2}\,r_a) \mod 4\mathcal{A}\ ;$$

on a $r_a = R_a + \frac{c-1}{2}$, d'où $-r_a^2 + cr_a - (1+s)\,\frac{f}{2}\,r_a = -R_a^2 + R_a + \frac{c^2-1}{4} - (1+s)\,\frac{f}{2}\,\frac{c-1}{2}$. Comme χ est pair et que $R_a = -R_a$ pour tout $a \in [1,f]'$, il vient

$$\begin{aligned} Y &\equiv 2 \sum_{a\in[1,\frac{f}{2}]'} \chi(a)(-R_a^2 + \frac{c^2-1}{4} - (1+s)\,\frac{f}{2}\,\frac{c-1}{2}) \\ &\equiv 2 \sum_{a\in[1,\frac{f}{2}]'} \chi(a)R_a \mod 4\mathcal{A}\,, \end{aligned}$$

car $\frac{c^2-1}{4} \equiv (1+s)\,\frac{f}{2}\,\frac{c-1}{2} \equiv 0 \mod 2$ et $R_a^2 \equiv R_a \mod 2$.

On a donc obtenu

$$B_f'^c = u_c A_f'^c \equiv (1-s)\langle\omega\chi^{-1}\langle\ \rangle^s, \nu_F'\rangle + s(1-s)fY' \mod 2s(1-s)f\mathcal{A}\,, \tag{1.5.4}$$

où $Y' = \sum_{a\in[1,\frac{f}{2}]'} \chi(a)R_a$.

On remarque alors que cette formule vaut pour tout p (cf. (1.5.3)).

D'après (1.5.1), on a à faire le rapprochement avec

$$u_c^{-1}(1-s)\langle\omega\chi^{-1}\langle\ \rangle^s, \nu_F^{+\prime\prime}\rangle \mod u_c^{-1}s(1-s)f\mathcal{A}\,,$$

où $\nu_F^{+\prime\prime} = \sum_{a\in[1,\frac{f}{2}]'} R_a\sigma_a^{-1}$. On a (cf. (1.3.6)) :

$$\begin{aligned} \langle\omega\chi^{-1}\langle\ \rangle^s, \nu_F'\rangle &= \sum_{a\in[1,f]'} \omega^{-1}\chi(a)\langle a\rangle^{-s}R_a \\ &= \sum_{a\in[1,\frac{f}{2}]'} (\omega^{-1}\chi(a)\langle a\rangle^{-s}R_a + \omega^{-1}\chi(f-a)\langle f-a\rangle^{-s}R_{f-a}) \\ &= \sum_{a\in[1,\frac{f}{2}]'} \omega^{-1}\chi(a)R_a(\langle a\rangle^{-s} + \langle a-f\rangle^{-s}) \\ &= \sum_{a\in[1,\frac{f}{2}]'} \omega^{-1}\chi(a)R_a\langle a\rangle^{-s}(1 + (1-a^{-1}f)^{-s})\,; \\ &\equiv 2 \sum_{a\in[1,\frac{f}{2}]'} \omega^{-1}\chi(a)\langle a\rangle^{-s}R_a \\ &\quad + sf \sum_{a\in[1,\frac{f}{2}]'} \omega^{-1}\chi(a)\langle a\rangle^{-s}a^{-1}R_a \mod 2sf\mathcal{A}\,; \end{aligned}$$

d'où, en remarquant que la seconde somme est à calculer modulo $2\mathcal{A}$ lorsque $p = 2$:

$$\begin{aligned} \frac{1}{2}\,\langle\omega\chi^{-1}\langle\ \rangle^s, \nu_F'\rangle &\equiv \sum_{a\in[1,\frac{f}{2}]'} \omega^{-1}\chi(a)\langle a\rangle^{-s}R_a + \frac{1}{2}\,sfY'' \mod sf\mathcal{A}\,, \\ &\equiv \langle\omega\chi^{-1}\langle\ \rangle^s, \nu_F^{+\prime\prime}\rangle + \frac{1}{2}\,sfY'' \mod sf\mathcal{A}, \end{aligned}$$

où $Y'' = \sum_{a\in[1,\frac{f}{2}]'} \omega^{-1}\chi(a)R_a$.

Ainsi, on obtient (cf. (1.5.1)) :

$$\frac{1}{2}(1-s)L_p(\chi,s) \equiv u_c^{-1}(1-s)\langle\omega\chi^{-1}\langle\ \rangle^s, \nu_F^{+\prime\prime}\rangle$$

$$\equiv u_c^{-1}(1-s)\ \frac{1}{2}\langle\omega\chi^{-1}\langle\ \rangle^s, \nu_F'\rangle - u_c^{-1}\ \frac{1}{2}\ s(1-s)fY''$$

$$\equiv u_c^{-1}\ \frac{1}{2}(u_c A_f'^c - s(1-s)fY') - u_c^{-1}\ \frac{1}{2}\ s(1-s)fY''$$

$$\equiv \frac{1}{2}\ A_f'^c - \frac{1}{2}\ s(1-s)fu_c^{-1}(Y'+Y'') \quad (\text{d'après (1.5.4)})$$

$$\equiv \frac{1}{2}\ A_f'^c \mod u_c^{-1}s(1-s)f\mathcal{A}$$

puisque $Y'+Y'' = \sum_{a\in[1,\frac{f}{2}]'} \chi(a)(1+\omega^{-1}(a))R_a \equiv 0 \mod 2\mathcal{A}$ si $p=2$;

d'où :

(1.5.5)
$$\frac{1}{2}(1-s)L_p(\chi,s) \equiv$$

$$\frac{1}{2}\sum_{a\in[1,f]'}\left(-\frac{a}{f}+\frac{1-s}{2}\right)\omega^{-1}\chi(a)\langle a\rangle^{-s} \mod u_c^{-1}s(1-s)f\mathcal{A}.$$

Etudions alors, modulo $u_c^{-1}s(1-s)f\mathcal{A}$, le terme résiduel

(1.5.6)
$$\frac{1}{4}(1-s)\sum_{a\in[1,f]'}\omega^{-1}\chi(a)\langle a\rangle^{-s}$$

ci-dessus. Pour effectuer les calculs modulo $u_c^{-1}s(1-s)f\mathcal{A}$, il faut estimer la somme ci-dessus

$$Z = \sum_{a\in[1,f]'}\omega^{-1}\chi(a)\langle a\rangle^{-s} \mod 4u_c^{-1}sf\mathcal{A}\ .$$

Calculons v_eZ, avec $v_e = 1-\omega^{-1}\chi(e)\langle e\rangle^{-s}$ pour e étranger à f convenable, et ceci modulo $4v_eu_c^{-1}sf\mathcal{A}$. En supposant la valuation de u_c minimale, on a à étudier $\frac{v_e}{u_c}$ en fonction du choix de e.

Supposons d'abord $p\neq 2$. Si $o(\chi)$ n'est pas puissance de p, $\psi = \omega^{-1}\chi$ a la même propriété (sinon ψ serait pair) ; dans ce cas $\frac{v_e}{u_c}\in\mathcal{A}^*$ pour e convenable . Si $o(\chi)=p^r$, $r\geq 0$, $o(\psi)$ n'est pas puissance de p et on a $\frac{v_e}{u_c}\in\frac{1}{\pi}\mathcal{A}^*$ (resp. $\frac{1}{(1-s)p}\mathcal{A}^*$) si $\chi\neq\chi_0$ (resp. $\chi=\chi_0$).

On a alors

$$v_eZ = \sum_{a\in[1,f]'}\omega^{-1}\chi(a)\langle a\rangle^{-s}(1-(1+a^{-1}r_a'f)^{-s}),$$

où $r_a' = r_a^e$, soit

$$v_e Z \equiv \sum_{a\in[1,f]'} \omega^{-1}\chi(a)\langle a\rangle^{-s}\, sa^{-1}r_a' f$$
$$\equiv 0 \mod sf\mathcal{A}$$

ce qui résoud le cas $p \neq 2$.

Supposons maintenant $p = 2$. Si $o(\chi)$ n'est pas d'ordre puissance de 2, $\psi = \omega^{-1}\chi$ a la même propriété et $\frac{v_e}{u_c} \in \mathcal{A}^*$ pour e convenable. Si χ et ψ sont d'ordre puissances de 2, il y a plusieurs cas :

(i) $o(\chi) = 2^r$, $r \geq 2$; alors $o(\psi) = o(\chi)$ et on peut choisir e de telle sorte que $\frac{v_e}{u_c} \in \mathcal{A}^*$;

(ii) $o(\chi) = 2$; comme $\psi = \omega^{-1}\chi \neq \chi_0$ (car χ est pair), $o(\psi) = 2$ et la conclusion est analogue ;

(iii) $\chi = \chi_0$, $\psi = \omega^{-1}$; on a $u_c = 1 - \langle c\rangle^{1-s} \in 4(1-s)\mathcal{A}^*$ et $v_e = 1 + \langle e\rangle^{-s} \in 2\mathcal{A}^*$ pour e tel que $\omega(e) = -1$; d'où $\frac{v_e}{u_c} \in \frac{1}{2(1-s)}\,\mathcal{A}^*$.

En résumé, dans le cas (i) et (ii) on a

$$4u_c^{-1}v_e sf\mathcal{A} = 4sf\mathcal{A},$$

dans le cas (iii), on a

$$4u_c^{-1}v_e sf\mathcal{A} = \frac{2s}{1-s}\, f\mathcal{A}.$$

On a alors :

$$v_e Z = \sum_{a\in[1,f]'} \omega^{-1}\chi(a)\langle a\rangle^{-s}(1-(1+a^{-1}r_a' f)^{-s})$$
$$\equiv sf \sum_{a\in[1,f]'} \omega^{-1}\chi(a)\langle a\rangle^{-s}(a^{-1}r_a' - \frac{1}{2}\,(1+s)a^{-2}r_a'^2 f) \mod 2sf^2\mathcal{A},$$

et par conséquent, il suffit de calculer la somme Z' ci-dessus modulo 4 (resp.2) si $\chi \neq \chi_0$ (resp. $\chi = \chi_0$).

Pour $\chi \neq \chi_0$, on a

$$Z' \equiv \sum_{a\in[1,f]'} \chi(a)r_a' - \frac{f}{2}\,(1+s) \sum_{a\in[1,f]'} \chi(a)r_a' \mod 4\mathcal{A} ;$$

or $\sum_{a\in[1,f]'} \chi(a)r_a' = \sum_{a\in[1,f]'} \chi(a)R_a' = 0$ par parité de χ et imparité de $R_a' = r_a' + \frac{1-e}{2}$.

Pour $\chi = \chi_0$, on a, modulo 2 :

$$Z' \equiv \sum_{a\in[1,f]'} \omega^{-1}(a)r_a' = \sum_{a\in[1,f]'} \omega^{-1}(a)R_a'$$
$$\equiv \sum_{a\in[1,f]'} R_a'$$
$$\equiv 0 \mod 2.$$

D'où le fait que (cf.(1.5.6)) :

$$\frac{1}{4}(1-s)\sum_{a\in[1,f]'}\omega^{-1}\chi(a)\langle a\rangle^{-s}\equiv 0 \mod u_c^{-1}s(1-s)f\mathcal{A}.$$

On a donc obtenu (cf.(1.5.5)) :

$$(1-s)\frac{1}{2}L_p(\chi,s)=-\frac{1}{2f}\sum_{a\in[1,f]'}\chi(a)\langle a\rangle^{1-s}+M'(s)X(s),$$

où $X(S)\in\mathcal{A}$ et où $M'(s)=s(1-s)f$, $s(1-s)\frac{f}{\pi}$, $\frac{sf}{q}$ selon la nature de $o(\chi)$.
Si l'on fait $s=-1$, il vient

$$\begin{aligned}M'(-1)X(-1)&=L_p(\chi,-1)+\frac{1}{2f}\sum_{a\in[1,f]'}\chi(a)\langle a\rangle^2\\&=L_p(\chi,-1)+\frac{1}{2f}\sum_{a\in[1,f]'}\omega^{-2}\chi(a)a^2\ ;\end{aligned}$$

or d'après (1.4)',

$$\begin{aligned}L_p(\chi,-1)&=-\frac{1}{2}B_2(\omega^{-2}\chi)\ (\text{ avec }\omega^{-2}\chi \mod f)\\&=-\frac{1}{2f}\sum_{a\in[1,f]'}\omega^{-2}\chi(a)(a^2-af+\frac{f^2}{6})\ \ (\text{cf.(IV.5.3 et 5.3.4)}),\end{aligned}$$

et il vient :

$$M'(-1)X(-1)=\frac{1}{2}\sum_{a\in[1,f]'}\omega^{-2}\chi(a)a-\frac{f}{12}\sum_{a\in[1,f]'}\omega^{-2}\chi(a)$$

$$=\frac{1}{2}\sum_{a\in[1,\frac{f}{2}]'}(\omega^{-2}\chi(a)a+\omega^{-2}\chi(f-a)(f-a))-\frac{f}{12}\sum_{a\in[1,f]'}\omega^{-2}\chi(a)$$

$$=\frac{f}{2}\sum_{a\in[1,\frac{f}{2}]'}\omega^{-2}\chi(a)-\frac{f}{12}\sum_{a\in[1,f]'}\omega^{-2}\chi(a).$$

(i) Cas où $\chi\neq\omega^2$. Dans ce cas, on a

$$0=\sum_{a\in[1,f]'}\omega^{-2}\chi(a)=2\sum_{a\in[1,\frac{f}{2}]'}\omega^{-2}\chi(a),$$

soit $M'(-1)X(-1)=0$. D'où $X(-1)=0$.

Si l'on écrit le développement de $X(s)$ en les puissances de $1+s$, on obtient (cf.(1.4.5)) :

$$X = x_0 + (1+s)X', \; X' \in \mathcal{A},$$

d'où ici $x_0 = 0$ et $X(s) \in (1+s)\mathcal{A}$, et le théorème dans ce cas.

(ii) Cas où $\chi = \omega^2$. Dans ce cas on a

$$\begin{aligned} M'(-1)X(-1) &= \frac{f}{2} \sum_{a \in [1, \frac{f}{2}]'} 1 - \frac{f}{12} \sum_{a \in [1,f]'} 1 \\ &= \frac{1}{4} f\varphi(f) - \frac{1}{12} f\varphi(f) = \frac{1}{6} f\varphi(f). \end{aligned}$$

On a donc $X(-1) = \frac{f\varphi(f)}{6M'(-1)}$ qui est aussi x_0 ; d'où :

(α) si $\omega^2 \neq \chi_0$, ce qui équivaut à $p \notin \{2,3\}$, on a $M'(s) = s(1-s)f$ et $M'(-1) = -2f$;

(β) si $\omega^2 = \chi_0$ et $p = 3$, on a $M'(s) = s\,\frac{f}{3}$ et $M'(-1) = -\frac{f}{3}$;

(γ) si $\omega^2 = \chi_0$ et $p = 2$, on a $M'(s) = s\,\frac{f}{4}$ et $M'(-1) = -\frac{f}{4}$.

D'où, respectivement :

$$x_0 = -\frac{\varphi(f)}{12}, -\frac{\varphi(f)}{2}, -\frac{2\varphi(f)}{3},$$

et

$$\begin{aligned} M'(s)X(s) &\equiv -\frac{1}{12} f\varphi(f)s(1-s) \mod s(1-s)(1+s)f\mathcal{A}, \\ &\equiv -\frac{1}{6} f\varphi(f)s \qquad \mod \frac{1}{3} s(1+s)f\mathcal{A}, \\ &\equiv -\frac{1}{6} f\varphi(f)s \qquad \mod \frac{1}{4} s(1+s)f\mathcal{A}, \end{aligned}$$

selon que $p \geq 5$, $p = 3$ ou $p = 2$.

Ceci achève la démonstration du théorème en donnant la valeur de $N(s)$ dans le cas particulier où $\chi = \omega^2$.

(1.6) **Corollaire**. Si $\chi = \chi_0$, $L_p(\chi_0, s)$ a un pôle simple en $s = 1$ dont le résidu est $1 - \frac{1}{p}$.

En effet, par (1.5), et pour $f = p^h$, $h \to \infty$, on a

$$\lim_{s \to 1} (s-1)\, L_p(\chi_0, s) \equiv \sum_{a \in [1,f]'} \frac{1}{f} = \frac{p^{h-1}(p-1)}{p^h} = 1 - \frac{1}{p} \mod p^{h-1};$$

d'où le résultat à la limite.

(1.7) **Corollaire**. En $s = 1$, et pour $\chi \neq \chi_0$, on a la formule d'approximation suivante :

$$\frac{1}{2} L_p(\chi, 1) \equiv \frac{-1}{2f} \sum_{a \in [1,f]'} \chi(a)\, log\, a \mod 2f \;\left(\text{resp.} \frac{2f}{\pi} \right)$$

si χ n'est pas (resp. est) d'ordre puissance de p.

D'après (1.5) et pour tout $s \neq 1$, on a

$$\frac{1}{2} L_p(\chi, s) \equiv -\frac{1}{2} \frac{1}{1-s} \frac{1}{f} \sum_{a \in [1,f]'} \chi(a)\langle a\rangle^{1-s} + \frac{N(s)}{1-s}$$

$$\equiv -\frac{1}{2f} \sum_{a \in [1,f]'} \chi(a) \frac{\langle a\rangle^{1-s} - 1}{1-s} + \frac{N(s)}{1-s} \mod \frac{M(s)}{1-s} ,$$

où l'on a pu remplacer $\langle a\rangle^{1-s}$ par $\langle a\rangle^{1-s} - 1$ puisque $\chi \neq \chi_0$.

Faisons tendre s vers 1 ; on a alors $\frac{\langle a\rangle^{1-s}-1}{1-s} \to log\ a$, d'où, dans le cas général où $\chi \neq \omega^2$:

$$\frac{1}{2} L_p(\chi, 1) \equiv \frac{-1}{2f} \sum_{a \in [1,f]'} \chi(a)\ log\ a \mod 2f \ (\text{ resp.} \frac{2f}{\pi})$$

si $o(\chi)$ n'est pas (resp. est) une puissance de p. Si $\chi = \omega^2$ (ce qui suppose $p \geq 5$ puisque $\chi \neq \chi_0$), le résultat est analogue puisque dans ces cas $\frac{N(s)}{1-s} = -\frac{1}{12} f\ \varphi(f) \equiv 0 \mod f$.

(1.8) **Remarque.** On se reportera au livre de Washington [W] pour l'expression de Leopoldt de la valeur $\frac{1}{2} L_p(\chi, 1)$ en termes de logarithmes p-adiques d'unités cyclotomiques. Cette formule, analogue à l'expression complexe de $\frac{1}{2} L(\chi, 1)$ (cf. [B–S]), ne permet cependant pas un calcul approché facile de $\frac{1}{2} L_p(\chi, 1)$, car les logarithmes en question (logarithmes de nombres algébriques non rationnels) s'approchent difficilement en pratique.

2.— Transformée de Mellin sur Δ_S.

On suppose toujours que S est un ensemble fini de nombres premiers contenant p.

(2.1) **Définition.** On considère l'application de G_S dans $\mathbb{Z}_p[G_S] \subset \Lambda_S$ qui à $\sigma \in G_S$ associe $N\sigma \cdot \sigma^{-1}$ (cf.(IV.2.3), (IV.2.4)) ; cette application (qui est continue) se prolonge par $\mathbb{Z}_p$-linéarité à $\mathbb{Z}_p[G_S]$, puis par continuité à Λ_S. Cette involution m sur la $\mathbb{Z}_p$-algèbre Λ_S s'appelle la transformée de Mellin des mesures. Comme l'image par m d'un élément non nul et non diviseur de 0 de Λ_S est de même nature, on peut prolonger m à Δ_S.

(2.2) **Remarque.** On a $m(\delta^\tau) = m(1 - N\tau \cdot \tau^{-1}) = 1 - \tau$. Supposons que δ^τ soit non nul et non diviseur de 0 dans Λ_S (ce qui équivaut à $\langle\tau\rangle \neq 1$), alors on sait aussi (cf. (IV.3.6.1)) que pour tout sous-corps K de $\mathbb{Q}(S)$, δ_K^τ est non nul et non diviseur de 0 (autrement dit, $(\delta^\tau)^{-1} \in \Delta_S'$). Par contre, $1 - \tau$ donne $1 - \tau_K$ par restriction, qui est nul ou diviseur de 0 dès que $[K : \mathbb{Q}] < \infty$ (bien que $1 - \tau$ soit non nul et non diviseur de 0 dans Λ_S). On prendra donc garde au fait que $m(\Delta_S')$ n'est pas contenu dans Δ_S'.

On a le résultat suivant qui se trouve admettre une généralisation complète au cas des fonctions L d'un corps totalement réel k (cf. [D–R]) :

(2.3) **Théorème.** La transformée de Mellin $DR_S = m(St_S)$ de la distribution de Stickelberger St_S (S contenant p) est une $\mathbb{Z}_p$-pseudo-mesure (cf.(II.6.2)) pour laquelle

$$L_p(\chi, s) = \langle \chi\langle\ \rangle^{1-s},\ DR_S \rangle ,$$

pour tout caractère de Dirichlet χ modulo S et tout $s \in \mathbb{Z}_p$, $s \neq 1$ si $\chi = \chi_0$.

démonstration

Soit $\sigma \in G_S$; montrer que
$(1-\sigma)DR_S \in \Lambda_S$ équivaut à montrer que $m(1-\sigma)m(DR_S) \in \Lambda_S$, soit que l'on a $(1 - N\sigma \cdot \sigma^{-1})St_S \in \Lambda_S$, ce qui provient d'une propriété fondamentale des distributions de Stickelberger : d'après (IV.3.4), on a

$$(1 - N\sigma \cdot \sigma^{-1})\rho_F \in \mathbb{Z}_p[G_F]$$

pour tout $F \in \mathcal{F}_S'$; par conséquent, sachant (par (IV.3.6)) que $\rho_F = \frac{\nu_F^\tau}{\delta^\tau}$ (avec δ^τ non nul et non diviseur de 0, ce qui n'est pas nécessairement le cas de $\delta^\sigma = 1 - N\sigma \cdot \sigma^{-1}$, σ parcourant G_S et pouvant être en particulier tel que $\langle\sigma\rangle = 1$), il vient :

$$(1 - N\sigma \cdot \sigma_F^{-1})\delta_F^\tau \rho_F = (1 - N\sigma \cdot \sigma_F^{-1})\nu_F^\tau \in \delta_F^\tau \, \mathbb{Z}_p[G_F] \, ,$$

soit, à la limite :

$$(1 - N\sigma \cdot \sigma^{-1})\nu_S^\tau \in \delta^\tau \Lambda_S \, ,$$

d'où $(1 - N\sigma \cdot \sigma^{-1})\frac{\nu_S^\tau}{\delta^\tau} \in \Lambda_S$.

On a donc bien un élément de $\widetilde{\Lambda}_S$.

La comparaison des intégrales est immédiate car pour $\sigma \in G_S$, on a :

$$\begin{aligned} \langle \chi\langle\ \rangle^{1-s}, m(\sigma)\rangle &= \langle \chi\langle\ \rangle^{1-s}, \omega(\sigma)\langle\sigma\rangle\sigma^{-1}\rangle \\ &= \omega(\sigma)\langle\sigma\rangle\chi^{-1}(\sigma)\langle\sigma\rangle^{s-1} \\ &= \langle \omega\chi^{-1}\langle\ \rangle^s, \sigma\rangle \, . \end{aligned}$$

(2.4) **Proposition.** Les pseudo-mesures DR_S (S contenant p) vérifient les propriétés eulériennes suivantes : Soient K, L, $K \subseteq L \subseteq \mathbb{Q}(S)$; on suppose que K contient $\mathbb{Q}(\{p\})$; alors par restriction de $\widetilde{\Lambda}_L$ à $\widetilde{\Lambda}_K$ (cf.(II.6.2)), on a :

$$DR_{L,K} = DR_K \prod_\ell \left(1 - \frac{1}{\ell}\, \sigma_{\ell,K}\right) \, ,$$

où ℓ parcourt l'ensemble des nombres premiers ramifiés dans $L/\mathbb{Q}$ et non ramifiés dans $K/\mathbb{Q}$.

Ceci résulte de (IV.4.6), compte-tenu du fait que pour pouvoir appliquer la transformation de Mellin m, il faut que le caractère N soit défini au moins sur $Gal(K/\mathbb{Q})$ et donc que K contienne $\mathbb{Q}(\{p\})$; on remarque alors que L/K est non ramifiée en p et p ne figure donc pas dans le produit ci-dessus.

(2.4.1) **Remarques.** (i) Puisque $p \in S$ et que S est fini on est dans le cas où G_S est de la forme (cf.(IV.1.7),(ii)) :

$$G_S = A_S \oplus \Gamma, \, \Gamma \simeq \mathbb{Z}_p, \, | \, A_S(p) \, | < \infty \, ;$$

on peut même utiliser une décomposition canonique en posant

$$A_S = Gal(\mathbb{Q}(S)/\mathbb{Q}_\infty),\ \Gamma = Gal(\mathbb{Q}(S)/\mathbb{Q}(S_0)(\mu_q)),\ S_0 = S - \{p\}\ .$$

(ii) Indépendamment de la transformée m, la restriction $\widetilde{\Lambda}_L \to \widetilde{\Lambda}_K$ ne peut exister que si le "dénominateur universel" des pseudo-mesures, à savoir $T = 1 - \gamma$, où γ est un pro-générateur de Γ, ne donne pas 0 ou un diviseur de 0 par restriction, ce qui suppose déjà que K contienne $\mathbb{Q}_\infty$.

D'après (III.3.4) et (2.4.1),(i), on peut énoncer :

(2.5) **Corollaire.** Il existe une constante $c_S \in \mathbb{Z}_p$ et une mesure $\mu_S \in \Lambda_{A_S}[[T]]$, tels que

$$DR_S = c_S \frac{\alpha_{A_S}}{T} + \mu_S\ ,$$

où α_{A_S} est la mesure de Haar sur A_S (cf.(II.4.3)).

Par intégration on en déduit les faits suivants :

(2.6) **Corollaire.** On a, pour χ primitif pair et $\mu_S = \sum_{i\geq 0} a_i T^i \in \Lambda_{A_S}[[T]]$:

(i) $L_p(\chi, s) = \sum_{i\geq 0} \langle \chi, a_i\rangle (1 - \chi(\gamma)\langle\gamma\rangle^{1-s})^i$ si χ n'est pas un caractère de $\mathbb{Q}_\infty$;

(ii) $L_p(\chi_r, s) = c_S \frac{qp^{-1}}{1-\chi_r(\gamma)\langle\gamma\rangle^{1-s}} + \sum_{i\geq 0} \langle \chi_0, a_i\rangle (1 - \chi_r(\gamma)\langle\gamma\rangle^{1-s})^i$,

si $\chi = \chi_r$ est un caractère de $\mathbb{Q}_\infty$ ($s \neq 1$ si $\chi_r = \chi_0$), où $S = \{p\}$;

(iii) $c_S = \prod_{\ell\in S} (1 - \frac{1}{\ell})^* \frac{log\ \langle\gamma\rangle}{q}$

où $(x)^*$ désigne l'unité $x\ p^{-v(x)}$ pour tout $x \in \mathbb{Q}_p^\times$.

Les points (i) et (ii) résultent de (II.5.6) appliqué à la restriction de χ à A_S. Le calcul de c_S, quel que soit S contenant p, se fait en recalculant le résidu de $\langle \chi_0\langle\ \rangle^{1-s},\ DR_S\rangle$ en $s = 1$; compte-tenu du fait qu'on a isolé une partie polaire de nature élémentaire, ce résidu est donné par

$$\lim_{s\to 1}\ c_S \mid A_S(p) \mid \frac{s-1}{1-\langle\gamma\rangle^{1-s}} = c_S \mid A_S(p) \mid \lim_{s\to 1} \left(\frac{\langle\gamma\rangle^{1-s} - 1}{1-s}\right)^{-1}$$
$$= c_S \frac{\mid A_S(p) \mid}{log\ \langle\gamma\rangle}\ ;$$

par ailleurs $\langle \chi_0\langle\ \rangle^{1-s},\ DR_S\rangle$ est $L_p(\chi_0, s)$ pour le caractère χ_0 considéré comme caractère modulo S et d'après (2.4) on a donc

$$\langle \chi_0\langle\ \rangle^{1-s},\ DR_S\rangle = \prod_{\substack{\ell\in S\\ \ell\neq p}} \left(1 - \frac{\langle\ell\rangle^{1-s}}{\ell}\right) \cdot \langle \chi_0\langle\ \rangle^{1-s},\ DR_{\{p\}}\rangle\ ;$$

d'où

$$c_S \frac{\mid A_S(p) \mid}{log\ \langle\gamma\rangle} = \prod_{\substack{\ell\in S\\ \ell\neq p}} \left(1-\frac{1}{\ell}\right) \cdot \lim_{s\to 1} (s-1)L_p(\chi_0,s)$$

$$= \prod_{\ell\in S} \left(1-\frac{1}{\ell}\right) \text{ (cf.(V.1.6))}.$$

On sait également que $\mid A_S \mid$ (au sens de (I.5.1)) est donné par

$$\mid A_S \mid = \varphi(q) \prod_{\substack{\ell\in S\\ \ell\neq p}} ((\ell-1)\ell^{\infty}) \ .$$

Désignons par $(x)_p$ la p-partie positive d'un rationnel x ; alors $\mid A_S(p) \mid = \prod_{\ell\in S} (\ell-1)_p$ (resp. $\mid A_S(2) \mid = 2 \prod_{\ell\in S} (\ell-1)_2$) ; d'où

$$c_S = \prod_{\ell\in S} \left(1-\frac{1}{\ell}\right) \prod_{\ell\in S} (\ell-1)_p^{-1} \frac{log\ \langle\gamma\rangle}{qp^{-1}},$$

ce qui s'écrit, en remarquant que $\frac{x}{(x)_p} = (x)^*$ et que $(\ell-1)_p = (1-\frac{1}{\ell})_p$ pour tout $\ell \neq p$:

$$c_S = \prod_{\ell\in S} \left(1-\frac{1}{\ell}\right)^* \frac{log\ \langle\gamma\rangle}{q} \in \mathbb{Z}_p^*.$$

(2.7) **Remarques**. (i) Ecrivons St_S sous la forme

$$St_S = (1-\sigma_{-1})St_S^+ \text{ (cf.(IV.4.8))} ;$$

alors $DR_S = m(St_S) = (1+\sigma_{-1})DR_S^-$, en remarquant que $m(\sigma_{-1}) = N\sigma_{-1}\cdot\sigma_{-1}^{-1} = -\sigma_{-1}$, et que DR_S^-, définie modulo l'idéal $(1-\sigma_{-1})T^{-1}\Lambda_S$, est une distribution de dénominateur $m(\delta^\tau) = 1-\tau$; on peut par exemple écrire :

$$St_S^+ = \frac{\nu_S^{\tau+}}{\delta^\tau}, \quad \nu_S^{\tau+} \in \Lambda_S \ ,$$

auquel cas

$$DR_S^- = \frac{m(\nu_S^{\tau+})}{m(\delta^\tau)} = \frac{\nu_S^{\tau-}}{1-\tau} \ , \quad \nu_S^{\tau-} \in \Lambda_S \ , \text{ définie mod } (1-\sigma_{-1})\Lambda_S.$$

(ii) On aura $1-\tau = T$ si l'on prend $\tau = \gamma$ générateur topologique de Γ.

Il résulte de ceci que l'on doit se poser le problème de savoir comment la décomposition (2.5) de DR_S est compatible avec ces questions de "parité" :

La réponse est donnée par le résultat suivant :

(2.8) **Proposition.** (i) Si $p \neq 2$, on a

$$DR_S = \frac{1}{2}\, c_S(1+\sigma_{-1})\alpha_{A_S} T^{-1} + (1+\sigma_{-1})\mu_S^- \ ,$$

où $\mu_S^- \in \Lambda_S$ est définie modulo $(1-\sigma_{-1})\Lambda_S$.

(ii) Si $p = 2$, on a

$$DR_S = c_S(1+\sigma_{-1})\alpha_{B_S} T^{-1} + (1+\sigma_{-1})\mu_S^- \ ,$$

où $B_S = Gal(\mathbb{Q}(S)/\mathbb{Q}(\{2\}))$ et μ_S^- comme en (i).

(iii) Par conséquent, on peut poser, modulo $(1-\sigma_{-1})T^{-1}\Lambda_S$:

$$DR_S^- = \frac{1}{2}\, c_S \alpha_{A_S} T^{-1} + \mu_S^- \ \ (\text{resp. } c_S \alpha_{B_S} T^{-1} + \mu_S^-) \ .$$

Supposons d'abord $p \neq 2$. Comme α_{A_S} est invariante par translation, on a $(1+\sigma_{-1})\alpha_{A_S} = 2\alpha_{A_S}$, d'où

$$DR_S = \frac{1}{2}\, c_S(1+\sigma_{-1})\alpha_{A_S} T^{-1} + \mu_S.$$

Par ailleurs, on a (cf.(2.7),(i)) :

$$DR_S = (1+\sigma_{-1})\nu_S^- T^{-1},\ \nu_S^- \in \Lambda_S$$

(en prenant $\tau = \gamma$ pour définir le dénominateur de St_S), d'où

$$\mu_S = (1+\sigma_{-1})(\nu_S^- T^{-1} - \frac{1}{2}\, c_S \alpha_{A_S} T^{-1}) \ .$$

Ecrivons $\mu_S = \sum_{i\geq 0} a_i T^i \in \Lambda_{A_S}[[T]]$ et $\nu_S^- = \sum_{i\geq 0} a_i^- T^i$ de même ; il vient, dans $\Lambda_{A_S} T^{-1} + \Lambda_{A_S}[[T]]$:

$$\mu_S = (1+\sigma_{-1})(a_0^- - \frac{1}{2}\, c_S \alpha_{A_S})T^{-1} + \sum_{i\geq 1} (1+\sigma_{-1}) a_i^- T^{i-1} \ ,$$

ce qui conduit à

$$(1+\sigma_{-1})(a_0^- - \frac{1}{2}\, c_S \alpha_{A_S}) = 0 \ \text{ et } a_i = (1+\sigma_{-1})a_{i+1}^- \ \text{ pour } i \geq 0 \ ;$$

d'où l'existence, modulo $(1-\sigma_{-1})\Lambda_S$, de

$$\mu_S^- = \sum_{i\geq 1} a_i^- T^{i-1} \ .$$

On notera que la 1ère relation donne $a_0^- \equiv \frac{1}{2}\, c_S \alpha_{A_S} \mod (1-\sigma_{-1})\Lambda_{A_S}$, ce qui était prévisible.

Le cas $p = 2$ est un peu plus subtil.

On a le résultat suivant :

(2.8.1) **Lemme.** On a la décomposition suivante :

$$A_S = B_S \oplus H_{-1} ,$$

où $H_{-1} = \langle \sigma_{-1} \rangle$ (d'ordre 2) et $B_S = Gal(\mathbb{Q}(S)/\mathbb{Q}(\{2\}))$.

Montrons d'abord que la conjugaison complexe σ_{-1} s'écrit

$$\sigma_{-1} = \prod_{\ell \in S} h_\ell^{(2)} ,$$

où $h_\ell^{(2)}$ désigne l'élément d'ordre 2 de $H_\ell = Gal(\mathbb{Q}(S)/\mathbb{Q}(S-\{\ell\}))$, sur la somme directe

$$A_S = \bigoplus_{\ell \in S} H_\ell .$$

Posons $\sigma_{-1} = \prod_{\ell \in S} h_\ell^{(2)x_\ell}$, $x_\ell \in \{0,1\}$, puisque σ_{-1} est d'ordre 2 ; par restriction aux corps $K_\ell = \mathbb{Q}(\{\ell\})$, on doit obtenir la conjugaison complexe sur ces corps ; or les groupes $Gal(K_\ell/\mathbb{Q}) \simeq \mathbb{Z}_\ell^*$ n'ont qu'un seul élément d'ordre 2, qui est $h_{\ell,K_\ell}^{(2)}$ et $\sigma_{-1,K_\ell} = h_{\ell,K_\ell}^{(2)x_\ell}$, d'où $x_\ell = 1$ pour tout ℓ.

Le lemme en résulte car on a $A_S = \bigoplus_{\ell \in S} H_\ell = B_S \oplus H_2$, et en écrivant le générateur $h_2^{(2)} = h_2$ de H_2 sous la forme

$$h_2 = \sigma_{-1} \prod_{\ell \in S-\{2\}} h_\ell^{(2)} ,$$

on en déduit que $B_S \oplus H_2 = B_S \oplus H_{-1}$.

(2.8.2) **Corollaire.** On a $\alpha_{A_S} = \alpha_{B_S}\ \alpha_{-1}$, où $\alpha_{-1} = 1 + \sigma_{-1}$ (mesure de Haar sur H_{-1}) et où α_{B_S} est la mesure de Haar sur B_S.

Ceci résulte de (II.4.6) appliqué à la décomposition du lemme.

Il vient alors, dans ce cas :

$$DR_S = c_S(1+\sigma_{-1})\alpha_{B_S} T^{-1} + \mu_S = (1+\sigma_{-1})\nu_S^- T^{-1} ,$$

et le raisonnement est ensuite analogue à celui du cas $p \neq 2$:
on peut écrire $\mu_S = (1+\sigma_{-1})\mu_S^-$, $\mu_S^- \in \Lambda_S$ définie modulo $(1-\sigma_{-1})\Lambda_S$.

Résumons les résultats obtenus dans l'énoncé suivant :

(2.9) **Théorème.** Soit S un ensemble fini de nombres premiers contenant p ; posons (cf.(2.6),(iii)) $c'_S = \frac{q}{2p}\, c_S$, à savoir

$$c'_S = \prod_{\ell \in S} \left(1 - \frac{1}{\ell}\right)^* \frac{log\ \langle\gamma\rangle}{2p} \in \mathbb{Z}_p^* \text{ dans tous les cas.}$$

Alors il existe une pseudo-mesure $DR_S^- \in \widetilde{\Lambda}_S$ de la forme

$$DR_S^- = c'_S \alpha_{A_S} T^{-1} + \mu_S^- \quad (\text{resp. } c'_S \alpha_{B_S} T^{-1} + \mu_S^-) ,$$

μ_S^- définie modulo $(1 - \sigma_{-1})\Lambda_S$, telle que (en termes de caractères primitifs) :

(i) $\frac{1}{2}\, L_p(\chi, s) = \langle \chi\langle\ \rangle^{1-s}, \mu_S^- \rangle$, si χ n'est pas caractère de $\mathbb{Q}_\infty$;

(ii) $\frac{1}{2}\, L_p(\chi, s) = c'_S(1 - \chi_r(\gamma)\langle\gamma\rangle^{1-s})^{-1} + \langle \chi_r\langle\ \rangle^{1-s}, \mu_S^- \rangle$,

si $\chi = \chi_r$ est caractère de $\mathbb{Q}_\infty$ ($s \neq 1$ si $r = 0$).

Par la suite nous utiliserons essentiellement cette formulation qui rend compte, de façon la plus précise possible, de certaines subtilités et qui présentent de façon unifiée les cas $p \neq 2$ et $p = 2$.

3.— Propriétés élémentaires de $\frac{1}{2}\, L_p(\chi, s)$.

Commençons par des résultats d'intégralité :

(3.1) **Théorème.** Soit $\chi \in tor(X^{ab})$, χ pair et primitif, et soit $\mathbb{Z}_p(\chi)$ l'anneau des valeurs de χ sur $\mathbb{Z}_p$. Alors pour tout $s \in \mathbb{Z}_p$ ($s \neq 1$ si $\chi = \chi_0$) on a

$$\frac{1}{2}\, L_p(\chi, s) \in \mathbb{Z}_p(\chi)$$

si et seulement si χ n'est pas caractère de $\mathbb{Q}_\infty$. Si $\chi = \chi_r$, $r \geq 1$, alors on a

$$\frac{1}{2}\, L_p(\chi_r, s) \in \frac{1}{\pi_r}\, \mathbb{Z}_p(\chi_r)^* + \mathbb{Z}_p(\chi_r) ,$$

où π_r est une uniformisante de $\mathbb{Z}_p(\chi_r)$. Si $\chi = \chi_0$, alors on a

$$\frac{1}{2}\, L_p(\chi_0, s) \in \frac{1}{q(1-s)}\, \mathbb{Z}_p^* + \mathbb{Z}_p,\ s \neq 1 .$$

démonstration

L'intégrale de $\chi\langle\ \rangle^{1-s}$ par rapport au terme polaire de DR_S^- est, d'après (2.9), non nulle si et seulement si $\chi = \chi_r$, $r \geq 0$; comme $\langle \chi\langle\ \rangle^{1-s}, \mu_S^- \rangle \in \mathbb{Z}_p(\chi)$, il reste à étudier la partie polaire pour $\chi = \chi_r$: elle est donnée par

$$\frac{c'_S}{1 - \chi_r(\gamma)\langle\gamma\rangle^{1-s}} = \frac{c'_S}{1 - \zeta_r\langle\gamma\rangle^{1-s}}$$

où ζ_r est une racine de l'unité d'ordre $p^r = o(\chi_r)$ puisque $\gamma_{\mathbb{Q}_\infty}$ est générateur topologique de $Gal(\mathbb{Q}_\infty/\mathbb{Q})$.

Si $r \neq 0$, $1 - \zeta_r\langle\gamma\rangle^{1-s} \equiv 1 - \zeta_r \mod q$, d'où le résultat avec $\pi_r = 1 - \zeta_r$. Si $r = 0$, on obtient $\frac{c_s}{1-\langle\gamma\rangle^{1-s}}$ qui est de la forme $\frac{u(s)}{q(1-s)}$, $u(s) \in \mathbb{Z}_p^*$, d'après (1.4.6).

(3.2) **Remarques**. (i) Désignons par v_χ la valuation normalisée sur $\mathbb{Q}_p(\chi)$ (si $\mathbb{Q}_p(\chi) = \mathbb{Q}_p$, on a $v_\chi = v$). On a $v_\chi(\frac{1}{2}\, L_p(\chi, s)) \geq 0$ si et seulement si χ n'est pas caractère de $\mathbb{Q}_\infty$; pour $r \geq 1$, $v_{\chi_r}(\frac{1}{2}\, L_p(\chi_r, s)) = -1$ pour tout $s \in \mathbb{Z}_p$; enfin $v(\frac{1}{2}\, L_p(\chi_0, s)) = -v(q) - v(1-s)$, pour tout $s \neq 1$.

(ii) Dans l'énoncé (3.1), on peut remplacer $\mathbb{Z}_p(\chi)$ (resp. $\mathbb{Z}_p^*$) par $\mathcal{A}$ (resp.$\mathcal{A}^*$) (cf.(1.4.5)).

On déduit de ce qui précède les informations correspondantes pour les nombres de Bernoulli ; une démonstration directe (par exemple celle qui figure déjà dans l'ancien livre de Hasse [H]) est toujours très compliquée, alors que le cadre présent des distributions fournit immédiatement le résultat :

(3.3) **Corollaire**. (i) Les nombres de Bernoulli $B_n(\chi)$ (cf.(IV.5.3)) χ pair, $n \geq 1$ impair, ont les propriétés suivantes (cf.(1.4)') ($\chi\omega^{-n}$ non nécessairement primitif) :

$v_\chi(\frac{1}{2n}\, B_n(\chi\omega^{-n})) \geq 0$ si χ n'est pas caractère de $\mathbb{Q}_\infty$,

$v_{\chi_r}(\frac{1}{2n}\, B_n(\chi_r\omega^{-n})) = -1$, pour tout $r \geq 1$,

$v(\frac{1}{2n}\, B_n(\omega^{-n})) = -v(q) - v(n)$.

(ii) En particulier, pour les nombres de Bernoulli d'indice 1 (ceux considérés déjà par Hasse pour les formules analytiques du nombre de classes relatives), on obtient :

$v_\chi(\frac{1}{2}\, B_1(\chi\omega^{-1})) \geq 0$ si χ n'est pas caractère de $\mathbb{Q}_\infty$,

$v_{\chi_r}(\frac{1}{2}\, B_1(\chi_r\omega^{-1})) = -1$ pour tout $r \geq 1$,

$v(\frac{1}{2}\, B_1(\omega^{-1})) = -v(q)$.

(3.4) **Remarques** (i) Dans l'énoncé ci-dessus, les caractères $\chi\omega^{-n}$ sont considérés comme caractères modulo S, l'ensemble formé des diviseurs premiers de f_χ et de p (les nombres de Bernoulli sont donc primitifs sauf dans le cas où le conducteur de $\chi\omega^{-n}$ est étranger à p (cf.(1.4.2))) ; on a donc $B_n(\chi\omega^{-n}) = (1 - (\chi\omega^{-n})'(p)p^{n-1})B_n((\chi\omega^{-n})')$, ce qui pose un problème de valuation uniquement lorsque $n = 1$ et lorsque $\psi = \chi\omega^{-1}$ est un caractère d'ordre puissance de p et de conducteur étranger à p. Mais dans ce cas, on a (cf.(IV.4.8) et (IV.5.4)) :

$$B_1(\psi) = -\langle\psi^{-1},\, St_{K_\psi}\rangle = -2\langle\psi^{-1},\, St^+_{K_\psi}\rangle,$$

où $St_{K_\psi} = St_{S_0,K_\psi} = \rho_{K_\psi}$, $S_0 = S - \{p\}$, ce qui fait que d'après (IV.3.6), $v_\psi(\frac{1}{2}\, B_1(\psi')) \geq 0$ (ψ étant impair, puisqu'on a supposé $n = 1$, on a $\psi \neq \chi_0$), ce qui complète (3.3).

(ii) Si l'on veut étudier de ce point de vue les nombres de Bernoulli ordinaires $B_n = B_n(\chi_0)$ (χ_0 modulo 1), il suffit d'écrire que

$$B_n = (1 - p^{n-1})^{-1}B_n(\psi_0), \text{ pour tout } n \geq 2,$$

où ψ_0 est le caractère unité modulo q ; on a alors

$$\frac{1}{2n} B_n = (1-p^{n-1})^{-1} \frac{1}{2n} B_n(\psi_0)$$
$$= (1-p^{n-1})^{-1} \frac{1}{2n} B_n(\omega^n \omega^{-n}),$$

soit

$$\frac{1}{2n} B_n = -(1-p^{n-1})^{-1} \frac{1}{2} L_p(\omega^n, 1-n),\ n \geq 2. \tag{3.4.1}$$

Si $n > 2$ est impair, ω^n est impair et on obtient $B_n = 0$ comme atttendu ; si $n \geq 2$ est pair, ω^n est pair et il y a 2 cas :

(α) $\omega^n \neq \chi_0$ (i.e. $n \not\equiv 0 \mod \varphi(q)$) :

On a alors $\frac{1}{2} L_p(\omega^n, 1-n) \in \mathbb{Z}_p(\omega) = \mathbb{Z}_p$, d'où :

$$v_p\left(\frac{1}{2} B_n\right) \geq v_p(n) \text{ pour tout } n \text{ pair } \geq 2,\ n \not\equiv 0 \mod \varphi(q). \tag{3.4.2}$$

(β) $\omega^n = \chi_0$ (i.e. $n \equiv 0 \mod \varphi(q)$) :

On a ici $v_p(\frac{1}{2} L_p(\chi_0, 1-n)) = -v(q) - v_p(n)$,
ce qui conduit à

$$v_p\left(\frac{1}{2} B_n\right) - v_p(n) = -v(q) - v_p(n).$$

Posons alors $n = m\varphi(q)$, $m \geq 1$; il vient :

$$v_p\left(\frac{1}{2} B_{m\varphi(q)}\right) = -v(q), \text{ pour tout } m \geq 1. \tag{3.4.3}$$

Par exemple, considérons $\frac{1}{2} B_2 \left(= \frac{1}{12}\right)$; pour $p = 2$, on obtient $v_2\left(\frac{1}{2} B_2\right)$ $= -2$ (par (3.4.3)) ; pour $p = 3$, on obtient $v_3\left(\frac{1}{2} B_{p-1}\right) = v_3\left(\frac{1}{2} B_2\right) = -1$ (par (3.4.3)), enfin pour tout $p > 3$, on a $\omega^2 \neq \chi_0$, ce qui donne $v_p\left(\frac{1}{2} B_2\right) \geq 0$ (par (3.4.2)). On a ainsi "reconstitué" le dénominateur de $\frac{1}{2} B_2$ qui doit donc être 12. On peut également introduire une fonction signe v_∞, dont on vérifie facilement qu'elle est définie par $v_\infty\left(\frac{1}{2} B_n\right) = (-1)^{\frac{n}{2}+1}$, pour tout $n \geq 2$.

Ceci se généralise ainsi : si l'on considère $\frac{1}{2} B_n$, $n \geq 2$ fixé, $v_p\left(\frac{1}{2} B_n\right)$ est négative si et seulement si $n \equiv 0 \mod \varphi(q)$; elle vaut alors $-v(q)$. D'où le dénominateur des $\frac{1}{2} B_n$, $n \geq 2$ pair.

Ecrivons $\frac{1}{2} B_n = \frac{b_n}{d_n}$, $(b_n, d_n) = 1$, $d_n > 0$; alors :

$$d_n = 4 \prod_{p-1 \mid n} p,\ n \text{ pair } \geq 2.$$

Par exemple, le dénominateur de $\frac{1}{2} B_{36}$ est égal à

$$4 \times 3 \times 5 \times 7 \times 13 \times 19 \times 37\ (= 3838380),$$

ce qui est confirmé par la table des nombres de Bernoulli de [W] (dans laquelle ceux-ci sont notés B_{2n} au lieu de B_n ; ainsi B_{36} est à lire pour $n = 18$).

Une façon encore plus directe d'obtenir une information sur le dénominateur de $\frac{1}{2} B_n$ est d'utiliser la congruence générale donnée par le théorème (1.5) :

On a :

$$\frac{1}{2} B_n = -(1-p^{n-1})^{-1} \cdot n \cdot \frac{1}{2} L_p(\omega^n, 1-n),\ n \geq 2,$$
$$\equiv +(1-p^{n-1})^{-1}\Big(\frac{1}{2f} \sum_{a \in [1,f]'} \omega^n(a)\langle a\rangle^n - N(1-n)\Big) \mod M(1-n),$$

où $f = q$; les résultats précédents d'intégralité montrent qu'il suffit d'étudier le cas où $\omega^n = \chi_0$ (i.e. $n \equiv 0 \mod \varphi(q)$) ; on a alors $M(1-n) \in \mathbb{Z}_p$ dans tous les cas.

Posons $\langle a\rangle = 1 + \lambda_a q$, $\lambda_a \in \mathbb{Z}_p$; on a

$$\frac{1}{2q} \sum_{a \in [1,q]'} \langle a\rangle^n \equiv \frac{1}{2q}\Big(\varphi(q) + nq \sum_a \lambda_a\Big) \mod \mathbb{Z}_p,$$

or pour $p = 2$, n étant pair, on obtient pour tout p :

$$\frac{1}{2} B_n \equiv (1-p^{n-1})^{-1}\Big(\frac{\varphi(q)}{2q} - N(1-n)\Big) \mod \mathbb{Z}_p.$$

Comme $\frac{\varphi(q)}{2q} = \frac{p-1}{2q} = \frac{p-1}{2p}$ (resp. $\frac{1}{4}$), que $N(1-n)$ est donné par 0 si $p \geq 5$, $-(1-n)$ si $p = 3$, $-\frac{4}{3}(1-n)$ si $p = 2$, il vient :

$$\frac{1}{2} B_n \equiv -\frac{1}{2p} \mod \mathbb{Z}_p \text{ (resp. } (1-2^{n-1})^{-1} \frac{1}{4} \mod \mathbb{Z}_2).$$

Dans le cas $p = 2$, $n = 2$, on a $\frac{1}{2} B_2 \left(= \frac{1}{12}\right) \equiv -\frac{1}{4} \mod \mathbb{Z}_2$; pour $n > 2$, on a $\frac{1}{2} B_2 \equiv \frac{1}{4} \mod \mathbb{Z}_2$.

On est donc amené à considérer $\frac{1}{2} B_n - \frac{1}{4} + \frac{1}{2} \sum_{\substack{p-1|n \\ p>2}} \frac{1}{p}$ qui est donc p entier pour tous les p intervenant dans le dénominateur de $\frac{1}{2} B_n$ (on vérifie que le résultat vaut pour $n = 1$ et 2) (*) :

(3.4.4) **Théorème** (congruences de von Staudt–Clausen). On a, pour tout n pair, $n \geq 2$ et pour $n = 1$: $\frac{1}{2} B_n - \frac{1}{4} + \frac{1}{2} \sum_{\substack{p, p>2 \\ p-1|n}} \frac{1}{p} \in \mathbb{Z}$.

(*) On obtient ainsi une amélioration des congruences de von Staudt–Clausen grâce à une étude plus précise en 2 ; il se trouve que la définition de $B_1 = \frac{1}{2}$ permet d'inclure le cas $n = 1$.

On notera que l'expression ci-dessus vaut 0 pour $n \leq 16$.

Malheureusement, c'est plutôt le numérateur des B_n qui a un intérêt en arithmétique (en direction du "théorème" de Fermat par exemple) ; or ce numérateur, qui croît très vite, est imprévisible. On a cependant des congruences classiques qui résultent de l'étude du module de continuité des fonctions L_p :

Soient s, $t \in \mathbb{Z}_p$; cherchons à estimer la différence

$$\frac{1}{2} L_p(\chi, s) - \frac{1}{2} L_p(\chi, t).$$

Si χ n'est pas caractère de $\mathbb{Q}_\infty$, on a d'après (2.9), en posant

$$\mu_S^- = \sum_{i \geq 0} a_i (1-\gamma)^i,\ a_i \in \Lambda_{A_S},$$

$$\frac{1}{2} L_p(\chi, s) = \sum_{i \geq 0} \chi(a_i)(1 - \chi(\gamma)\langle\gamma\rangle^{1-s})^i;$$

on peut supposer que $\langle\gamma\rangle = 1 + qu$, $u \in \mathbb{Z}_p^*$, d'où

$$1 - \chi(\gamma)\langle\gamma\rangle^{1-s} \equiv 1 - \chi(\gamma) + q(1-s)u' \mod qp\mathbb{Z}_p \ \text{(cf. (1.4.6))}, u' = u\chi(\gamma),$$

ce qui conduit à :

$$\frac{1}{2}\,L_p(\chi,s)-\frac{1}{2}\,L_p(\chi,t)\equiv$$

$$\equiv\sum_{i\geq 0}\chi(a_i)\Big((1-\chi(\gamma)+q(1-s)u')^i-(1-\chi(\gamma)+q(1-t)u')^i\Big)$$

$$\equiv 0 \mod q(s-t)\mathbb{Z}_p.$$

Si $\chi=\chi_r$, $r\geq 1$, le terme polaire intervient et on a en posant $\chi_r(\gamma)=\zeta_r$:

$$\frac{1}{1-\chi_r(\gamma)\langle\gamma\rangle^{1-s}}-\frac{1}{1-\chi_r(\gamma)\langle\gamma\rangle^{1-t}}=\frac{1-\zeta_r\langle\gamma\rangle^{1-t}-1+\zeta_r\langle\gamma\rangle^{1-s}}{(1-\zeta_r\langle\gamma\rangle^{1-s})(1-\zeta_r\langle\gamma\rangle^{1-t})}$$

$$\in\frac{q(s-t)}{\pi_r^2}\,\mathbb{Z}_p^* \quad (\pi_r=1-\zeta_r),$$

puisque $\zeta_r(\langle\gamma\rangle^{1-s}-\langle\gamma\rangle^{1-t})\equiv\zeta_r\ q\ u(t-s) \mod qp$.

Enfin si $\chi=\chi_0$, il vient

$$\frac{1}{1-\langle\gamma\rangle^{1-s}}-\frac{1}{1-\langle\gamma\rangle^{1-t}}\in\frac{q(s-t)}{q(1-s)q(1-t)}\,\mathbb{Z}_p^*$$

$$\in\frac{s-t}{q(1-s)(1-t)}\,\mathbb{Z}_p^*.$$

D'où l'énoncé correspondant :

(3.5) **Théorème**. Soit χ primitif pair d'ordre fini ; alors si χ n'est pas caractère de $\mathbb{Q}_\infty$,on a, pour tout $s,t\in\mathbb{Z}_p$:

$$\frac{1}{2}\,L_p(\chi,s)-\frac{1}{2}\,L_p(\chi,t)\equiv 0 \mod q(s-t)\mathbb{Z}_p\ ;$$

si $\chi=\chi_r$, $r\geq 1$, on a :

$$\frac{1}{2}\,L_p(\chi_r,s)-\frac{1}{2}\,L_p(\chi_r,t)\equiv 0 \mod \frac{q(s-t)}{\pi_r^2}\,\mathbb{Z}_p\ ;$$

si $\chi=\chi_0$, on a :

$$q(1-s)(1-t)\big(\frac{1}{2}\,L_p(\chi_0,s)-\frac{1}{2}\,L_p(\chi_0,t)\big)\equiv 0 \mod (s-t)\mathbb{Z}_p\ .$$

(3.6) **Remarques.** (i) La théorie des genres analytique (cf. [G1],[G2]) permet d'améliorer les divisibilités et congruences précédentes, au moins pour certains types de caractères (cf. par exemple [Pi]). Cette théorie repose sur le théorème de structure concernant les mesures eulériennes.

(ii) Appliquons ceci par exemple aux nombres de Bernoulli ordinaires (les autres cas se traitant de façon analogue) ; la relation (cf. (3.4.1)) :

$$\frac{1}{2n}\, B_n = -(1-p^{n-1})^{-1}\, \frac{1}{2}\, L_p(\omega^n, 1-n),\ n \geq 2,$$

ne peut être utilisée, pour comparer 2 tels nombres B_n, B_m, que pour $m \equiv n \mod \varphi(q)$ (afin d'avoir la même fonction L_p). Dans ce cas on a

$$(1-p^{n-1})\, \frac{B_n}{2n} - (1-p^{m-1})\, \frac{B_m}{2m} = \frac{1}{2}\, L_p(\omega^m, 1-m) - \frac{1}{2}\, L_p(\omega^n, 1-n).$$

Distinguons plusieurs cas (toujours avec $m \equiv n \mod \varphi(q)$) :

α) m, $n \geq 2$, pairs, non nuls modulo $\varphi(q)$.

On est dans le 1$^{\text{er}}$ cas du théorème, soit :

$$(3.6.1) \qquad (1-p^{n-1})\, \frac{B_n}{2n} - (1-p^{m-1})\, \frac{B_m}{2m} \equiv 0 \mod q(m-n)\mathbb{Z}_p.$$

Comme d'après (3.4.2) $\frac{B_n}{2n}$ et $\frac{B_m}{2m}$ sont p-entiers, on en déduit que pour $p \neq 2$ (le cas $p = 2$ n'ayant pas lieu) on a :

$$(3.6.2) \qquad \frac{B_n}{2n} \equiv \frac{B_m}{2m} \mod p\mathbb{Z}_p \ (m \equiv n \mod p-1,\ m, n \geq 2,\ m, n \not\equiv 0 \mod p-1).$$

Ces congruences s'appellent les congruences de Kummer et leur preuve directe n'est pas immédiate (voir une telle preuve dans [B–S]). On remarque que si, de plus, $n \equiv m \mod p^h$ (i.e. $n \equiv m \mod p^h(p-1)$) la congruence (3.6.1) s'améliore d'autant.

Par exemple on a $\frac{B_{10}}{10} \equiv \frac{B_4}{4} \mod 7$ (on utilise [W] pour le vérifier, en faisant attention au fait que les signes n'y sont pas indiqués) : ici, il faut calculer modulo 7 :

$$\frac{1}{30 \times 7} + \frac{5}{6 \times 10} = \frac{1}{4}\, \frac{63}{30 \cdot 33} \equiv 0 \mod 7.$$

β) $n \equiv m \equiv 0 \mod \varphi(q)$.

Il vient alors, en utilisant le 3$^{\text{ème}}$ cas du théorème :

$$(3.6.1)' \qquad q(1-p^{n-1})m\, \frac{B_n}{2} - q(1-p^{m-1})n\, \frac{B_m}{2} =$$

$$= qmn\Big(\frac{1}{2}\, L_p(\chi_0, 1-m) - \frac{1}{2}\, L_p(\chi_0, 1-n)\Big) \equiv 0 \mod (m-n)\ ;$$

autrement dit, dans ce cas on a seulement une relation d'intégralité en p (sauf si en plus $m \equiv n \mod p^h$, $h \geq 1$). D'après (3.4.3), on a $v(\frac{1}{2} B_n) = -v(q)$, donc $q \frac{B_n}{2}$ et $q \frac{B_m}{2}$ sont p-entiers et on peut alors écrire en particulier :

$$(3.6.2)' \qquad q\, m \frac{B_n}{2} - q\, n \frac{B_m}{2} \in \mathbb{Z}_p .$$

Par exemple, pour $p = 3$, $n = 2$, $m = 8$, on a (par $(3.6.1)'$) :

$$48(1-3)\frac{B_2}{2} - 12(1-3^7)\frac{B_8}{2} \equiv 0 \mod 6\mathbb{Z}_3 ,$$

soit

$$-48B_2 - 6B_8 \equiv 0 \mod 3$$

soit

$$16B_2 + 2B_8 \in \mathbb{Z}_3 ;$$

or $B_2 = \frac{1}{6}$, $B_8 = -\frac{1}{30}$ et $16B_2 + 2B_8 = \frac{13}{5} \in \mathbb{Z}_3$.

(3.7) **Remarque**. Les principes précédents se généralisent dans de nombreuses directions et devraient permettre de retrouver, d'une manière unifiée, les nombreuses congruences connues et les nouvelles établies par Urbanowicz dans [U1], [U2], [U3] ; donnons-en un simple exemple qui indique parfaitement la méthode à suivre :

Fixons, pour $r \geq 2$, r valeurs distinctes $s_1, \ldots, s_r \in \mathbb{Z}_p$ et considérons une expression de la forme

$$(3.7.1) \qquad A = \sum_{j=1}^{r} c_j \frac{1}{2} L_p(\chi, s_j),\ c_j \in \mathbb{C}_p ,$$

en supposant pour simplifier χ non caractère de $\mathbb{Q}_\infty$.
D'après (2.9), (i), si $\mu_S^- = \sum_{i \geq 0} a_i T^i \in \Lambda_{A_S}[[T]]$, $T = 1 - \gamma$, on a pour $s \in \mathbb{Z}_p$:

$$\frac{1}{2} L_p(\chi, s) = \sum_{i \geq 0} \chi(a_i)(1 - \chi(\gamma)\langle\gamma\rangle^{1-s})^i ;$$

posons $1 - \langle\gamma\rangle^{1-s} = q(s)$; il vient alors :

$$\begin{aligned} \frac{1}{2} L_p(\chi, s) &= \sum_{i \geq 0} \chi(a_i)(1 - \chi(\gamma) + \chi(\gamma)q(s))^i \\ &= \sum_{i \geq 0} \chi(a_i)(1 - \chi(\gamma))^i + \sum_{i \geq 1} \alpha_i q(s)^i , \end{aligned}$$

où la 1ère série, notée α_0, est convergente puisque $(1-\chi(\gamma))^i \to 0$, et où les α_i sont dans $\mathbb{Z}_p(\chi)$ et indépendants de s. D'où :

$$\frac{1}{2}\, L_p(\chi,s) = \sum_{i\geq 0} \alpha_i q(s)^i,\ \alpha_i \in \mathbb{Z}_p(\chi),\ q(s) = 1 - \langle\gamma\rangle^{1-s}\ . \tag{3.7.2}$$

On a donc

$$A = \sum_{i\geq 0} \alpha_i \sum_{j=1}^{r} c_j\ q(s_j)^i\ ,$$

et une façon universelle d'avoir des congruences est d'imposer les k conditions :

$$\sum_{j=1}^{r} c_j\ q(s_j)^i = 0, \quad i = 0,\dots,k-1\ ,$$

avec k maximum ; on aura alors

$$A \equiv 0 \mod \Big(\sum_{j=1}^{r} c_j q(s_j)^{k+i}\Big)_{i\geq 0}\ ,$$

soit au moins, si les c_j sont entiers :

$$A \equiv 0 \mod q^k\ .$$

Si $\sum_{j=1}^{r} c_j(1-\langle\gamma\rangle^{1-s_j})^i = 0$, $i = 0,\dots,k-1$, ceci est équivalent à

$$\sum_{j=1}^{r} c_j(\langle\gamma\rangle^{1-s_j})^i = 0,\ i = 0,\dots,k-1\ . \tag{3.7.3}$$

Si $k \geq r$, le système homogène ci-dessus n'admet que la solution nulle ; pour $k = r-1$, on peut fixer $c_r = -1$ par exemple et on obtient explicitement les valeurs des c_j et la congruence suivante dans $\mathbb{Z}_p(\chi)$:

$$\sum_{j=1}^{r} c_j\ \frac{1}{2}\ L_p(\chi,s_j) \equiv 0 \mod \Big(\sum_{j=1}^{r} c_j q(s_j)^{r-1+i}\Big)_{i\geq 0}\ ; \tag{3.8}$$

on remarque aussi (cf.(3.7.3)) que le problème est invariant par translation du r-uple $(s_1,\dots,s_r)$ par une constante de $\mathbb{Z}_p$, c'est-à-dire que l'on a, pour tout $t \in \mathbb{Z}_p$:

$$\sum_{j=1}^{r} c_j\ \frac{1}{2}\ L_p(\chi,s_j+t) \equiv 0 \mod \Big(\sum_{j=1}^{r} c_j q(s_j+t)^{r-1+i}\Big)_{i\geq 0}\ .$$

(3.8.1) **Exemples.** (i) Pour $r = 2$, on obtient la condition $c_1 + c_2 = 0$ qui correspond au cas de l'étude du module de continuité de $\frac{1}{2} L_p(\chi, s)$ (cf.(3.5)).

(ii) Pour $r = 3$, on obtient, pour $c_3 = -1$:

$$\begin{cases} c_1 + c_2 = 1 \\ c_1\langle\gamma\rangle^{1-s_1} + c_2\langle\gamma\rangle^{1-s_2} = \langle\gamma\rangle^{1-s_3} , \end{cases}$$

ce qui conduit à

$$c_1 = \frac{\langle\gamma\rangle^{1-s_2} - \langle\gamma\rangle^{1-s_3}}{\langle\gamma\rangle^{1-s_2} - \langle\gamma\rangle^{1-s_1}}, \quad c_2 = 1 - c_1, \quad c_3 = -1 .$$

On peut toujours supposer que $\langle\gamma\rangle = 1 + q$, et on est amené à utiliser (1.4.6) pour le calcul des c_j.

Prenons alors le triplet $(0, -1, 1)$ de valeurs de s ; on a

$$c_1 = \frac{2+q}{1+q}, \; c_2 = \frac{-1}{1+q}, \; c_3 = -1 .$$

On a alors, pour $i \geq 0$:

$$\begin{aligned} \sum_{j=1}^{3} c_j q(s_j)^{2+i} &= c_1(-q)^{2+i} + c_2(-2q - q^2)^{2+i} + c_3 \times 0 \\ &= \frac{2+q}{1+q}\, q^2(-q)^i - \frac{1}{1+q}\, q^2(2+q)^2(2+q)^i(-q)^i \\ &= \frac{q^2(2+q)}{1+q}\,(-q)^i(1 - (2+q)^{i+1}) \end{aligned}$$

qui, pour $i = 0$, donne

$$-q^2(2+q)$$

et un multiple pour tout $i \geq 1$. Le module de la congruence est donc :

$$p^2 \quad \text{si } p \neq 2, \quad 32 \quad \text{si } p = 2 .$$

On obtient donc :

$$\frac{2+q}{1+q}\,\frac{1}{2}\,L_p(\chi, 0) - \frac{1}{1+q}\,\frac{1}{2}\,L_p(\chi, -1) - \frac{1}{2}\,L_p(\chi, 1) \equiv 0 \; (q^2(2+q)) ;$$

comme $p\,\frac{1}{2}\,L_p(\chi, -1) - p\,\frac{1}{2}\,L_p(\chi, 0) \equiv 0 \mod p^2$ pour $p \neq 2$ (cf. (3.5)), on obtient finalement :

(3.8.2) **Théorème.** Soit χ un caractère pair d'ordre fini, non caractère de $\mathbb{Q}_\infty$. Alors on a les congruences suivantes :

$$2 \times \frac{1}{2}\,L_p(\chi, 0) - \frac{1}{2}\,L_p(\chi, -1) - \frac{1}{2}\,L_p(\chi, 1) \equiv 0 \mod p^2 \text{si } p \neq 2,$$

$$6 \times \frac{1}{2}\, L_2(\chi,0) - \frac{1}{2}\, L_2(\chi,-1) - 5 \times \frac{1}{2}\, L_2(\chi,1) \equiv 0 \mod 32.$$

On peut déduire de cette congruence une congruence reliant les différents invariants arithmétiques associés aux corps K_χ et $K_{\omega^{-1}\chi}$, au moins dans le cas $p = 2$ et χ quadratique impair :

Soit $\mathbb{Q}(\sqrt{d})$, $d > 0$, le corps K_χ supposé distinct de $\mathbb{Q}(\sqrt{2})$, soient $h(d)$, $\varepsilon(d)$, D le nombre de classes, l'unité fondamentale, le discriminant de $\mathbb{Q}(\sqrt{d})$, soit $k_2(d)$ le nombre d'éléments du K_2 de l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$, et enfin soit $h(-d)$ le nombre de classes de $\mathbb{Q}(\sqrt{-d})$; alors :

(3.8.3) **Corollaire.** On a la congruence :

$$3(1-\omega^{-1}\chi(2))h(-d) - \frac{2\chi(2)-1}{4w(d)}\, k_2(d) - 5(2-\chi(2))h(d)\frac{log\ \varepsilon(d)}{D} \equiv 0\ (32)\ ,$$

où $w(d) = 1$ sauf si $d = 5$ pour lequel on a $w(5) = 5$.

Ceci permet d'estimer $k_2(d)$ modulo 128 en fonction de $h(-d)$, $h(d)$, $\varepsilon(d)$.

Si par exemple 2 est décomposé dans $\mathbb{Q}(\sqrt{-d})$ (i.e. $\omega^{-1}\chi(2) = 1$), on obtient :

$$\frac{2\chi(2)-1}{4w(d)}\, k_2(d) \equiv 5(\chi(2)-2)\ h(d)\ \frac{log\ \varepsilon(d)}{D}\ (32)\ .$$

(3.9) **Cas des caractères d'ordre puissance de** p. Soit χ pair tel que $o(\chi) = p^r$; on peut supposer χ non caractère de $\mathbb{Q}_\infty$ en vertu de (3.1). Soient $S = \{\ell, \ell \text{ premier }, \ell \mid f_\chi\} \cup \{p\}$ et $S_0 = S - \{p\}$.

Pour $\sigma \in G_S$, on a $\chi\langle\ \rangle^{1-s}(\sigma) \equiv \chi_0\langle\ \rangle^{1-s}(\sigma) \mod (\pi)$, où π est une uniformisante de $\mathbb{Z}_p(\chi)$; par $\mathbb{Z}_p$-linéarité et par densité, on en déduit que $\langle\chi\langle\ \rangle^{1-s},\ \mu\rangle \equiv \langle\chi_0\langle\ \rangle^{1-s},\ \mu\rangle \mod (\pi)$ pour tout $\mu \in \Lambda_S$. Comme

$$\frac{1}{2}\, L_p(\chi,s) = \langle\chi\langle\ \rangle^{1-s},\ \mu_S^-\rangle\ ,$$

où l'on a posé $DR_S^- = c_S'\ \alpha\ T^{-1} + \mu_S^-$, $\alpha = \alpha_{A_S}$ (resp. α_{B_S}), $\mu_S^- \in \Lambda_{A_S}[[T]]$ (cf. (2.9)), il vient :

$$\frac{1}{2}\, L_p(\chi,s) \equiv \langle\chi_0\langle\ \rangle^{1-s},\ \mu_S^-\rangle \mod (\pi)\ ;$$

on a alors $\langle\chi_0\langle\ \rangle^{1-s},\ \mu_S^-\rangle = \langle\chi_0\langle\ \rangle^{1-s},\ \mu_{S,\mathbb{Q}_\infty}^-\rangle$ et

$$\begin{aligned}\mu_{S,\mathbb{Q}_\infty}^- &= DR_{S,\mathbb{Q}_\infty}^- - c_S'\ \alpha_{\mathbb{Q}_\infty}\ T_{\mathbb{Q}_\infty}^{-1} \\ &= \prod_{\ell\in S_0} (1-\ell^{-1}\sigma_{\ell,\mathbb{Q}_\infty})\ \cdot DR_{\mathbb{Q}_\infty}^- - c_S' \mid B_S(p) \mid T_{\mathbb{Q}_\infty}^{-1}\end{aligned} \tag{3.9.1}$$

(cf.(2.4) appliquée à $K = \mathbb{Q}(\{p\})$ avant restriction à $\mathbb{Q}_\infty$).

On aura $\frac{1}{2}\,L_p(\chi,s) \in \mathbb{Z}_p(\chi)^*$ si et seulement si $\langle \chi_0\langle\ \rangle^{1-s},\ \mu_S^-\rangle \in \mathbb{Z}_p(\chi)^*$, condition qui ne dépend pas du choix de s (on pourra par exemple travailler avec $s=0$) :

(i) Cas $p \neq 2$. On obtient :

$$\langle \chi_0\langle\ \rangle,\ \mu_S^-\rangle = \prod_{\ell\in S_0}(1-\omega^{-1}(\ell))\cdot\frac{1}{2}\,L_p(\chi_0,0) - c_S'\prod_{\ell\in S_0}(\ell-1)_p\cdot\,(1-\langle\gamma\rangle)^{-1}\,.$$

On a $S_0 \neq \emptyset$ en raison des hypothèses faites, et comme tout $\ell \neq p$ ramifié dans $K_\chi/\mathbb{Q}$ est $\equiv 1 \mod p$, le 1er terme est nul ; comme $(1-\langle\gamma\rangle)^{-1} \in \frac{1}{p}\,\mathbb{Z}_p^*$, on a

$$\langle \chi_0\langle\ \rangle,\ \mu_S^-\rangle \in \frac{1}{p}\prod_{\ell\in S_0}(\ell-1)_p\,\mathbb{Z}_p^*\,. \tag{3.9.2}$$

(ii) Cas $p=2$. On a de même $S_0 \neq \emptyset$, mais on n'a pas nécessairement la condition $\omega(\ell)=1$ (par exemple si χ est le caractère quadratique de conducteur 21). On a :

$$\frac{1}{2}\,L_2(\chi,0) \equiv \langle \chi_0\langle\ \rangle,\ \mu_{S,\mathbb{Q}_\infty}^-\rangle \mod(\pi)\ ;$$

or, comme dans le cas (i), on a :

$$\begin{aligned}\mu_{S,\mathbb{Q}_\infty}^- &= DR_{S,\mathbb{Q}_\infty}^- - c_S'\alpha_{\mathbb{Q}_\infty}T_{\mathbb{Q}_\infty}^{-1}\\ &= \prod_{\ell\in S_0}(1-\ell^{-1}\sigma_{\ell,\mathbb{Q}_\infty}^-)DR_{\mathbb{Q}_\infty}^- - c_S'\mid B_S(2)\mid(1-\gamma_{\mathbb{Q}_\infty})^{-1}\ ;\end{aligned}$$

et

$$DR_{\mathbb{Q}_\infty}^- = c_{\{p\}}'T_{\mathbb{Q}_\infty}^{-1} + \mu_{\{p\},\mathbb{Q}_\infty}^-\ .$$

En choisissant par exemple γ tel que $\langle\gamma\rangle = 5$, il vient :

$$\langle \chi_0\langle\ \rangle,\ \mu_{S,\mathbb{Q}_\infty}^-\rangle \equiv -\frac{1}{4}\,c_{\{p\}}'\prod_{\ell\in S_0}(1-\omega^{-1}(\ell)) + \frac{1}{4}\,c_S'\prod_{\ell\in S_0}(\ell-1)_2 \mod(\pi)\,,$$

où $c_{\{p\}}' = \frac{log\,\langle\gamma\rangle}{4}$ et $c_S' = \prod_{\ell\in S_0}(1-\ell^{-1})^*\cdot\frac{log\,\langle\gamma\rangle}{4}$ (cf.(2.9)),

ce qui conduit à

$$\langle \chi_0\langle\ \rangle,\ \mu_{S,\mathbb{Q}_\infty}^-\rangle \equiv \frac{1}{4}\,\frac{log\,\langle\gamma\rangle}{4}\Big(\prod_{\ell\in S_0}(1-\ell^{-1}) - \prod_{\ell\in S_0}(1-\omega^{-1}(\ell))\Big) \mod(\pi)\,.$$

Si $|S_0| > 2$, on a $\prod(1-\ell^{-1}) \equiv \prod(1-\omega^{-1}(\ell)) \equiv 0 \mod 8$ et $\langle \chi_0\langle\ \rangle,\ \mu_{S,\mathbb{Q}_\infty}^-\rangle \equiv 0 \mod(\pi)$.

Si $|S_0| = 1$, on a $1-\ell^{-1}-(1-\omega^{-1}(\ell)) \equiv \langle\ell\rangle^{-1}-1 \mod 8$.

Si $|S_0| = 2$, on a

$$(1-\ell_1^{-1})(1-\ell_2^{-1}) - (1-\omega^{-1}(\ell_1))(1-\omega^{-1}(\ell_2))$$
$$= \omega^{-1}(\ell_1) - \ell_1^{-1} + \omega^{-1}(\ell_2) - \ell_2^{-1} - (\omega^{-1}(\ell_1)\omega^{-1}(\ell_2) - \ell_1^{-1}\ell_2^{-1})$$
$$= \omega^{-1}(\ell_1)(1-\langle\ell_1\rangle^{-1}) + \omega^{-1}(\ell_2)(1-\langle\ell_2\rangle^{-1}) - \omega^{-1}(\ell_1\ell_2)(1-\langle\ell_1\ell_2\rangle^{-1})$$
$$\equiv 1-\langle\ell_1\rangle^{-1} + 1 - \langle\ell_2\rangle^{-1} - (1-\langle\ell_1\ell_2\rangle^{-1})$$
$$\equiv (\langle\ell_1\rangle^{-1}-1)(\langle\ell_2\rangle^{-1}-1)$$
$$\equiv 0 \mod 8 ;$$

d'où $\langle\chi_0(\ ),\mu^-_{S,\mathbb{Q}_\infty}\rangle \equiv 0 \bmod (\pi)$ sauf si $|\ S_0\ | = 1$ où l'on a :

$$\langle\chi_0(\ ),\ \mu^-_{S,\mathbb{Q}_\infty}\rangle \in \frac{1}{4}(\langle\ell\rangle^{-1}-1)\mathbb{Z}_2^* \text{ si } S_0 = \{\ell\}\ . \tag{3.9.3}$$

En tenant compte de (3.9.2) et (3.9.3) on obtient le résultat suivant :

(3.9.4) **Théorème.** Soit χ un caractère pair d'ordre puissance de p ; alors $\frac{1}{2}\ L_p(\chi,s) \in \mathbb{Z}_p(\chi)^*$ (condition qui ne dépend pas de $s \in \mathbb{Z}_p$) si et seulement si le conducteur de χ est de la forme $p^r.\ell$, ℓ premier tel que $v_p(\ell-1) = 1$ (resp. $v_2(\langle\ell\rangle - 1) = 2$).

(3.9.5) **Remarque.** Ce résultat a été énoncé pour la première fois dans [R] ; la généralisation de ce type de résultat constitue la théorie analytique des genres dont les principaux résultats sont donnés dans [G1] et [G2].

(3.10) **Invariants d'Iwasawa analytiques.** Soit $\chi \in tor(X^{ab})$, χ pair. Pour tout $r \geq 0$, on considère les caractères $\chi\chi_r$, où χ_r est un caractère d'ordre p^r de $\mathbb{Q}_r$, et les nombres $\frac{1}{2}\ L_p(\chi\chi_r,s)$.

En utilisant (2.9) pour $S = \{\ell,\ \ell$ premier $,\ell \mid f_\chi\} \cup \{p\}$, on peut écrire :

$$DR_S^- = \sum_{i\geq -1} a_i T^i,\ a_i \in \Lambda_{A_S},\ T = 1-\gamma\ ,$$

où $a_{-1} = c'_S\alpha_{A_S}$ (resp. $c'_S\alpha_{B_S}$) ; décomposons alors le caractère χ sous la forme $\chi = \psi\chi'_{r_0}$ où χ'_{r_0} est un caractère de $\mathbb{Q}_\infty$ et où ψ est un caractère de A_S (i.e. un caractère du corps $\mathbb{Q}(S_0)\mathbb{Q}(\mu_q)$, $S_0 = S - \{p\}$) ; alors on a $\{\chi\chi_r,\ \chi_r$ caractère de $\mathbb{Q}_\infty\} = \{\psi\chi_r,\ \chi_r$ caractère de $\mathbb{Q}_\infty\}$ et il revient au même d'étudier les $\frac{1}{2}\ L_p(\psi\chi_r,s)$:

$$\frac{1}{2}\ L_p(\psi\chi_r,s) = \sum_{i\geq -1} \psi(a_i)(1-\chi_r(\gamma)\langle\gamma\rangle^{1-s})^i\ .$$

Dès que $r \geq 1$, $1-\chi_r(\gamma)\langle\gamma\rangle^{1-s} = \pi_r(s)$ est de valuation 1 dans $\mathbb{Z}_p(\chi_r)$, indépendamment de s. Ecrivons alors, dans $\mathbb{Z}_p(\psi)$, $\psi(a_i) = \varpi^{h_i}u_i$, $h_i \geq 0$, $u_i \in \mathbb{Z}_p(\psi)^*$, où ϖ est une uniformisante de $\mathbb{Z}_p(\psi)$; on a

$$\frac{1}{2}\ L_p(\psi\chi_r,s) = \sum_{i\geq -1} \varpi^{h_i}\ u_i\ \pi_r(s)^i\ .$$

Soient alors :

(3.10.1) $$\mu_\psi = \mathrm{Min}\{h_i,\ i \geq 1\} \text{ et } \lambda_\psi = \mathrm{Min}\{i \geq -1,\ h_i = \mu_\psi\}\ ;$$

on a $\mu_\psi \in \mathbb{N}$ et $\lambda_\psi \in [-1, \infty[$. Il est clair que si l'on considère la valuation $v_r = v_{\psi\chi_r}$ sur $\mathbb{Z}_p(\psi\chi_r)$, on a, pour tout r assez grand :

(3.10.2) $$v_r\big(\frac{1}{2}\ L_p(\psi\chi_r, s)\big) = \mu_\psi p^{r-r_0} + \lambda_\psi\ ,$$

où p^{r_0} est la p-partie de $o(\psi)$.

Un résultat important de la théorie des fonctions L p-adiques de $\mathbb{Q}$ est le suivant :

(3.10.3) **Théorème** (Ferrero-Washington, cf. [W]). On a $\mu_\psi = 0$ pour tout ψ.

(3.10.4) **Définition.** L'invariant λ_ψ s'appelle l'invariant d'Iwasawa analytique pour ψ ; on a par définition $\lambda_\psi = \lambda_{\psi\chi_r}$ pour tout caractère χ_r de $\mathbb{Q}_\infty$.

(3.10.5) **Remarques.** (i) Les formules analytiques du nombre de classes des corps abéliens imaginaires permettent alors de démontrer facilement, pour tout corps abélien imaginaire F, la formule d'Iwasawa, à savoir que la p-partie du nombre de classes relatives de $F\mathbb{Q}_n$ est de la forme $p^{\lambda^- n + \nu^-}$, pour tout n assez grand, où $\lambda^- \in \mathbb{N}$ et $\nu^- \in \mathbb{Z}$.

(ii) On a $\lambda_{\chi_r} = -1$ pour tout caractère χ_r de $\mathbb{Q}_\infty$ (cf. (3.1)) (i.e. $\lambda_{\chi_0} = -1$), et on a $\lambda_\chi \in \mathbb{N}$ dans tous les autres cas.

(3.10.6) **Exercice.** *Montrer que si l'on écrit ψ sous la forme $\psi = \psi_0\psi_p$, avec $(o(\psi_0), p) = 1$, $o(\psi_p) = p^r$, $r \geq 0$, on a :*

$$\lambda_\psi = \lambda_{\psi_0} + \sum_\ell\ p^{n(\ell)}\ (\ell | f_\psi,\ \ell \neq p,\ \psi_0(\ell) = 1)\ ,$$

où $p^{n(\ell)} = \big(\frac{\langle \ell \rangle - 1}{q}\big)_p$ (on pourra remarquer que, si l'on écrit $\frac{1}{2}\ L_p(\psi, s) = \langle \psi \langle\ \rangle^{1-s},\ \mu_S^- \rangle$ (cf. (2.9)), où $\mu_S^- = \sum_{i \geq 0}\ a_i T^i \in \Lambda_{A_S}[[T]]$, alors on a, pour h assez grand et n convenable :

$$\langle \psi\chi_{n+h} \langle\ \rangle^{1-s},\ \mu_S^- \rangle^{p^n} \equiv \langle \psi_0\chi_h \langle\ \rangle^{1-s},\ \mu_S^- \rangle \mod p\mathbb{Z}_p(\psi\chi_{n+h})\ ,$$

le résultat provenant de l'utilisation convenable de (2.4)).

4.— Terme polaire des distributions de Stickelberger.

Ayant identifié la décomposition de la pseudo-mesure DR_S^- (cf. (2.9)) sous la forme

$$DR_S^- = c_S' \, \alpha_{A_S} \, T^{-1} + \mu_S^- \ (\text{ resp. } c_S' \, \alpha_{B_S} T^{-1} + \mu_S^-), \, p \in S \ ,$$

on peut utiliser la transformée de Mellin pour décrire $St_S = m(DR_S)$, ou plutôt $St_S^+ = m(DR_S^-)$ qui s'écrit

$$St_S^+ = c_S' m(\alpha_{A_S}) m(T)^{-1} + m(\mu_S^-)$$

$$(\text{resp. } c_S' m(\alpha_{B_S}) m(T)^{-1} + m(\mu_S^-)) \ .$$

Si $T = 1 - \gamma$, $m(T) = 1 - N\gamma \cdot \gamma^{-1} = \delta^\gamma = 1 - \langle\gamma\rangle\gamma^{-1}$ (non nul et non diviseur de 0 dans Λ_S).

Examinons $m(\alpha_{A_S})$ (resp. $m(\alpha_{B_S})$) ; si $\sigma \in A_S$, $m(\sigma) = \omega(\sigma)\sigma^{-1}$ puisque $A_S = Ker(\langle\ \rangle)$:

(4.1) (i) cas $p \neq 2$. On a

$$A_S = \bigoplus_{\ell \in S} H_\ell, \quad \text{où } H_\ell = Gal(\mathbb{Q}(S)/\mathbb{Q}(S - \{\ell\})) \ \text{ si } \ell \neq p,$$

(4.1.1)

$$H_p = Gal(\mathbb{Q}(S)/\mathbb{Q}_\infty \, \mathbb{Q}(S - \{p\})) \ ;$$

d'où $\alpha_{A_S} = \prod_{\ell \in S} \alpha_{H_\ell}$ et $m(\alpha_{A_S}) = \prod_{\ell \in S} m(\alpha_{H_\ell})$.

Pour $\ell \neq p$, $H_\ell \subseteq Ker\ \omega$ et par conséquent $m(\alpha_{H_\ell}) = \alpha_{H_\ell}$ (l'involution $\sigma \to \sigma^{-1}$ invariant les mesures de Haar comme on le vérifie facilement sur les formules (II.4.3)) ; si $\ell = p$, H_p est cyclique d'ordre $p-1$, auquel cas $\alpha_{H_p} = \frac{1}{p-1} \sum_{\tau \in H_p} \tau$ (cf. (II.4.4)), d'où :

$$m(\alpha_{H_p}) = \frac{1}{p-1} \sum_{\tau \in H_p} \omega(\tau)\tau^{-1} = \frac{1}{p-1} \sum_{\tau \in H_p} \omega^{-1}(\tau)\tau \ . \tag{4.1.2}$$

Finalement, si l'on pose, par analogie avec le cas $p = 2$:

$$B_S = Gal(\mathbb{Q}(S)/\mathbb{Q}(\{p\})) \ , \tag{4.1.3}$$

il vient $A_S = B_S \oplus H_p$, $B_S = \oplus_{\ell \in S - \{p\}} H_\ell$, d'où

$$m(\alpha_{A_S}) = \alpha_{B_S} \, \frac{1}{p-1} \sum_{\tau \in H_p} \omega^{-1}(\tau)\tau \ . \tag{4.1.4}$$

(4.2) (ii) cas $p = 2$. Le raisonnement est le même pour les $m(\alpha_{H_\ell})$, $\ell \neq 2$, donc ici on a directement

$$m(\alpha_{B_S}) = \alpha_{B_S} \ , \tag{4.2.1}$$

où l'on a comme en (4.1.3) :

$$B_S = Gal(\mathbb{Q}(S)/\mathbb{Q}(\{2\})) \ . \tag{4.2.2}$$

Finalement, on peut énoncer :

(4.3) **Théorème.** Soit $\delta_0 = \delta^\gamma$ le dénominateur de la distribution de Stickelberger St_S, S contenant p, formé à partir de $\tau = \gamma$ générateur topologique de $\Gamma = Gal(\mathbb{Q}(S)/\mathbb{Q}(S - \{p\})\mathbb{Q}(\mu_q))$. Alors il existe une mesure $\mu_S^+ \in \Lambda_{A_S}[[\delta_0]]$ telle que

$$St_S^+ = c_S' \ \alpha_{B_S} \ \frac{1}{p-1} \left(\sum_{h \in H_p} \omega^{-1}(h) h \right) \delta_0^{-1} + \mu_S^+ \quad \text{si } p \neq 2,$$

$$St_S^+ = c_S' \ \alpha_{B_S} \ \delta_0^{-1} + \mu_S^+ \quad \text{si } p = 2.$$

(4.4) **Remarques.** (i) On voit que la méthode impose un δ_0 particulier, ce qui est normal car pour que les séries $\sum_{i \geq 0} \chi(a_i)\chi(\delta^\tau)^i$ convergent, il est nécessaire que $\chi(\delta^\tau) = 1 - \chi(\tau)\langle\tau\rangle^{1-s}$ ne soit pas inversible, donc que $o(\chi(\tau))$ soit une puissance de p pour tout χ, donc que $o(\tau) = p^\infty$.

(ii) Le terme polaire de St_S^+ est canonique bien que St_S^+ soit définie modulo $(1 + \sigma_{-1})\Lambda_S \delta_0^{-1}$.

(iii) On rappelle que l'unité p-adique c_S' (cf. (2.9)) dépend du choix de γ.

(iv) D'après (IV.4.1), on a le droit de restreindre les distributions St_S^+, par exemple de $\mathbb{Q}(S)$ à $\mathbb{Q}(S_0)$, $S_0 = S - \{p\}$, car alors $1 - \langle\gamma\rangle\gamma^{-1}$ donne $1 - \langle\gamma\rangle \neq 0$. On a en particulier (cf. (IV.4.6)) :

$$St_{S,S_0}^+ = (1 - \sigma_{p,S_0}^{-1}) St_{S_0}^+ \mod (1 + \sigma_{-1,S_0})\delta_{0,S_0}^{-1} \Lambda_{S_0} \ .$$

(v) On remarque que dans toute restriction de $\mathbb{Q}(S)$ à L telle que L ne contienne pas $\mathbb{Q}(\mu_q)$, le terme polaire de St_S^+ donne 0 pour $p \neq 2$ (car $\sum_{h \in H_p} \omega^{-1}(h) h_L = 0$ dans ce cas). Ce phénomène est cohérent avec l'étude des §§, 5, 6 suivants où l'on va pouvoir exhiber directement les corps L pour lesquels les distributions St_L sont des $\mathbb{Z}_p$-mesures ; le comportement particulier de 2 provenant du terme $\frac{1}{2} \sum_{a \in [1,f]'} \sigma_a^{-1}$ des éléments de Stickelberger.

5.— Critère d'intégralité des éléments de Stickelberger.

Soit F un corps abélien imaginaire de conducteur f, et soit S l'ensemble des nombres premiers ramifiés dans $F/\mathbb{Q}$.

On a $\rho_F = \sum_{a \in [1,f]'} \left(-\frac{a}{f} + \frac{1}{2} \right) \sigma_{a,F}^{-1} \in \mathbb{Z}[G_F]$ si et seulement si ρ_F est ℓ-entier pour tout $\ell \in S$ et pour $\ell = 2$ si $2 \notin S$. Pour étudier la ℓ-intégralité de ρ_F pour $\ell \in S$, on considère St_S pour le nombre premier $p = \ell$ et on rappelle qu'alors $St_{S,F} = \rho_F$.

Il est commode d'introduire une valuation notée encore v_p :

$$v_p : \mathbb{Q}[G_F] \longrightarrow \mathbb{Z} \cup \{\infty\} ,$$

ainsi définie : si $\rho = \sum_{\sigma \in G_F} a_\sigma \sigma$ est l'écriture de $\rho \in \mathbb{Q}[G_F]$ sur la base canonique, on pose

$$v_p(\rho) = \operatorname{Min}_\sigma(v_p(a_\sigma)) .$$

Comme ρ_F est somme d'un terme polaire (obtenu comme élément de $\mathbb{Q}[G_F]$ par restriction de celui de St_S) et d'un élément de $\mathbb{Z}_p[G_F]$, $v_p(\rho_F)$ est égale à la valuation du terme polaire de ρ_F lorsque celle-ci est < 0, sinon on a seulement $v_p(\rho_F) \geq 0$. Le terme polaire de ρ_F est alors (cf. (2.8) et (4.3)) :

$$(5.1) \qquad \alpha_{B_S,F} \sum_{h \in H_p} \omega^{-1}(h) h_F \delta_{0,F}^{-1} \text{ (à une unité p – adique près)} ,$$

où $\delta_0 = 1 - \langle\gamma\rangle\gamma^{-1}$ et où $\langle\gamma\rangle \in 1 + q\mathbb{Z}_p^*$.

Posons $\beta_F = \sum_{h \in H_p} \omega^{-1}(h) h_F$ et introduisons le sous-corps $F_0 = F \cap \mathbb{Q}(\{p\})$ de F pour lequel on pose $G_F^0 = Gal(F/F_0)$. On doit donc calculer la quantité :

$$(5.2) \qquad V_p = v_p(\alpha_{B_S,F}\ \beta_F\ \delta_{0,F}^{-1}) ,$$

qui est telle que

$$(5.2.1) \qquad v_p(\rho_F) = V_p \text{ si } V_p < 0, v_p(\rho_F) \geq 0 \text{ sinon} .$$

(5.2.2) **Remarque.** La valuation v_p n'est pas additive (il suffit par exemple de considérer σ d'ordre n et de remarquer que $(1-\sigma)(1+\sigma+\cdots+\sigma^{n-1}) = 0$). Cependant, si $\alpha \in \mathbb{Q}$, $\beta \in \mathbb{Q}[G_F]$, on a $v_p(\alpha\beta) = v_p(\alpha) + v_p(\beta)$.

On remarque que $\alpha_{B_S,F}$ est une mesure invariante par translation dans $\mathbb{Z}_p[G_F]$: en effet, si $\sigma_F \in G_F^0$, on peut relever σ_F en $\sigma \in B_S$ et il vient $\alpha_{B_S,F}\ \sigma_F = (\alpha_{B_S}\sigma)_F = \alpha_{B_S,F}$; elle est donc de la forme

$$\alpha_{B_S,F} = c_F\ \alpha_F^0 ,$$

où α_F^0 est la mesure de Haar sur G_F^0 et où $c_F \in \mathbb{Z}_p$ est donné par

$$\frac{|\ B_S(p)\ |}{|\ G_F^0(p)\ |} = \frac{1}{([F:F_0])_p} \prod_{\ell \in S-\{p\}} |\ H_\ell(p)\ | ;$$

or $|\ H_\ell(p)\ | = (\ell - 1)_p$ pour tout $\ell \neq 2$ et si $\ell = 2 \in S - \{p\}$, on a encore

$| H_2(p) | = (\ell - 1)_p$; d'où :

$$c_F = \frac{1}{([F : F_0])_p} \prod_{\ell \in S - \{p\}} (\ell - 1)_p \ . \tag{5.3}$$

On a donc $V_p = v_p(c_F\ \alpha_F^0\ \beta_F\ \delta_{0,F}^{-1})$ dans $\mathbb{Q}[G_F]$.
Posons :

$$\theta_F = 1 + \langle\gamma\rangle\gamma_F^{-1} + \cdots + \langle\gamma\rangle^{p^r-1}\ \gamma_F^{-(p^r-1)} \ ,$$

où $p^r = o(\gamma_F)$. Comme $\delta_{0,F}\ \theta_F = 1 - \langle\gamma\rangle^{p^r} \in qp^r\ \mathbb{Z}_p^*$, $\delta_{0,F}$ et θ_F sont non nuls et non diviseurs de 0, et on a (cf. (5.2.2)) :

$$V_p = v_p(c_F\ \alpha_F^0\ \beta_F\ \theta_F) - (r + 1 + v_p(2)) \ . \tag{5.4}$$

Soit Ω un système exact de représentants de G_F modulo G_F^0 ; alors tout $\eta \in \mathbb{Z}_p[G_F]$ s'écrit de façon unique :

$$\eta = \sum_{\sigma,\tau} a_{\sigma,\tau}\ \sigma\tau,\ \sigma \in \Omega,\ \tau \in G_F^0,\ a_{\sigma,\tau} \in \mathbb{Z}_p \ ,$$

et on a

$$\alpha_F^0\ \eta = \sum_{\sigma,\tau} a_{\sigma,\tau}\ \sigma\alpha_F^0 = \sum_{\sigma} A_\sigma\ \sigma\alpha_F^0, \text{où } A_\sigma = \sum_{\tau} a_{\sigma,\tau} \in \mathbb{Z}_p \ .$$

On observe alors que $v_p(\alpha_F^0\ \eta) = \operatorname{Min}_{\sigma}(v_p(A_\sigma))$.

Pour calculer A_σ, il revient au même de restreindre η à F_0 car $\eta_{F_0} = \sum_{\sigma,\tau} a_{\sigma,\tau}\ \sigma_{F_0} = \sum_{\sigma} (\sum_{\tau} a_{\sigma,\tau})\sigma_{F_0}$. En appliquant ceci à $\eta = c_F\ \beta_F\ \theta_F$, il vient :

$$\eta_{F_0} = c_F\ \beta_{F_0}\ \theta_{F_0}, \text{ où } \beta_{F_0} = \sum_{h \in H_p} \omega^{-1}(h)h_{F_0},\ \theta_{F_0} = \sum_{j=0}^{p^r-1} \langle\gamma\rangle^j \gamma_{F_0}^{-j} \ .$$

Or $\beta_{F_0} = 0$ dès que l'image de H_p dans G_{F_0} n'est pas d'ordre $\varphi(q)$ (i.e. $F_0\mathbb{Q}_\infty \subsetneq \mathbb{Q}(\{p\})$) ; il y a donc, pour $p = 2$, le cas particulier où F_0 est l'un des sous-corps imaginaires cycliques ne contenant pas $\sqrt{-1}$), pour $p \neq 2$ la condition étant équivalente à $\mathbb{Q}(\mu_p) \subseteq F_0$.

Commençons par le cas où $\mathbb{Q}(\mu_q) \subseteq F_0$:

Comme $o(\gamma_{F_0}) = p^{r_0} \geq 1$, et que γ_{F_0} fixe $\mathbb{Q}(\mu_q)$, on peut décomposer $Gal(F_0/\mathbb{Q})$ sous la forme :

$$Gal(F_0/\mathbb{Q}) = \overline{H}_p \oplus \overline{\Gamma} \ ,$$

où $\overline{H}_p \simeq Gal(\mathbb{Q}(\mu_q)/\mathbb{Q})$, $\overline{\Gamma} = Gal(F_0/\mathbb{Q}(\mu_q))$, $| \overline{\Gamma} | = p^{r_0}$; on a alors $\beta_{F_0} \in \mathbb{Z}_p[\overline{H}_p]$, $\theta_{F_0} \in \mathbb{Z}_p[\overline{\Gamma}]$, auquel cas l'interprêtation de $c_F\ \beta_{F_0}\theta_{F_0}$ dans $\mathbb{Z}_p[\overline{\Gamma}][\overline{H}_p]$ permet d'en déduire facilement que

$$V_p = v_p(c_F\ \theta_{F_0}) - (r + 1 + v_p(2)) \ .$$

Posons $j = \lambda p^{r_0} + k$, $0 \leq k < p^{r_0}$, $0 \leq \lambda < p^{r-r_0}$; alors

$$\theta_{F_0} = \sum_{\lambda,k} \langle\gamma\rangle^{\lambda p^{r_0}} \langle\gamma\rangle^{k} \gamma_{F_0}^{-k} = \sum_{k} \left(\langle\gamma\rangle^{k} \sum_{\lambda} \langle\gamma\rangle^{\lambda p^{r_0}} \right) \gamma_{F_0}^{-k} \in \mathbb{Z}_p[\overline{\Gamma}].$$

Posons $\langle\gamma\rangle^{p^{r_0}} = 1 + qp^{r_0}u_0$, $u_0 \in \mathbb{Z}_p^*$; il vient :

$$\sum_{\lambda=0}^{p^{r-r_0}-1} \langle\gamma\rangle^{\lambda p^{r_0}} = \frac{(1+qp^{r_0}u_0)^{p^{r-r_0}} - 1}{1 + qp^{r_0}u_0 - 1} \in p^{r-r_0}\,\mathbb{Z}_p^* ;$$

d'où

$$\begin{aligned} V_p &= v_p(c_F\, p^{r-r_0}) - (r + 1 + v_p(2)) \\ &= v_p(c_F) - (r_0 + 1 + v_p(2)) \\ &= v_p\left(\prod_{\ell \in S - \{p\}} (\ell - 1)_p \right) - v_p([F : F_0]qp^{r_0}) \text{ (cf.(5.3.3))}; \end{aligned}$$

comme $(|\, \overline{H}_p \,||\, \overline{\Gamma}\,|)_p = qp^{r_0-1}$, on en déduit que

$$v_p([F : F_0]qp^{r_0}) = v_p(p[F : \mathbb{Q}])$$

et donc que

$$V_p = v_p\left(\prod_{\ell \in S - \{p\}} (\ell - 1) \right) - v_p(p[F : \mathbb{Q}]) .$$

Dans le cas particulier évoqué relativement à $p = 2$, on a

$$\eta_{F_0} = c_F\, \beta_{F_0}\, \theta_{F_0}$$

avec

$$\beta_{F_0} = 1 - h_{F_0},\ \theta_{F_0} = \sum_{j=0}^{2^r-1} \langle\gamma\rangle^{j}\, \gamma_{F_0}^{-j} .$$

Posons pour simplifier $\gamma_{F_0} = \tau$; on a alors, en posant $[F_0 : \mathbb{Q}] = 2^{r_0}$ (qui est aussi égal à l'ordre de γ_{F_0}), $h_{F_0} = \tau^{2^{r_0-1}}$, et, comme dans le cas général,

$$\begin{aligned} \theta_{F_0} &= \sum_{j=0}^{2^r-1} \langle\gamma\rangle^{j}\, \tau^{-j} \\ &= \sum_{k=0}^{2^{r_0}-1} \left(\langle\gamma\rangle^{k} \sum_{\lambda=0}^{2^{r-r_0}-1} \langle\gamma\rangle^{\lambda 2^{r_0}} \right) \tau^{-k} . \end{aligned}$$

Par conséquent, les coefficients de $\beta_{F_0}\, \theta_{F_0}$, sur la base canonique de $\mathbb{Z}_2[G_{F_0}]$, sont donnés par :

$$\langle\gamma\rangle^{k} \sum_{\lambda=0}^{2^{r-r_0}-1} \langle\gamma\rangle^{\lambda 2^{r_0}} - \langle\gamma\rangle^{k \pm 2^{r_0-1}} \sum_{\lambda=0}^{2^{r-r_0}-1} \langle\gamma\rangle^{\lambda 2^{r_0}}$$

$$= \langle\gamma\rangle^k (1 - \langle\gamma\rangle^{\pm 2^{r_0-1}}) \frac{\langle\gamma\rangle^{2^{r_0}.2^{r-r_0}} - 1}{\langle\gamma\rangle^{2^{r_0}} - 1}$$

$$\in 4.2^{r_0-1} \frac{4.2^r}{4.2^{r_0}} \mathbb{Z}_2^*$$

$$= 2^{r+1} \mathbb{Z}_2^*.$$

Dans ce cas, on a (compte-tenu du fait que $[F_0 : \mathbb{Q}] = 2[F \cap \mathbb{Q}_\infty : \mathbb{Q}]$) :

$$V_2 = v_2\Big(\prod_{\ell \in S-\{2\}} (\ell - 1)\Big) - v_2([F : F_0]) + r + 1 - (r + 1 + 1)$$

$$= v_2\Big(\prod_{\ell \in S-\{2\}} (\ell - 1)\Big) + v_2([F \cap \mathbb{Q}_\infty : \mathbb{Q}]) - v_2([F : \mathbb{Q}]) .$$

Il reste à examiner la 2-intégralité lorsque $2 \notin S$. Dans ce cas, on a $\rho_F = \sum_{a \in [1,f]'} \Big(-\frac{a}{f} + \frac{1}{2}\Big)\sigma_{a,F}^{-1}$ qui est non 2-entier si et seulement si $\frac{1}{2} \sum_{a \in [1,f]'} \sigma_{a,F}^{-1}$ n'est pas 2-entier, soit si et seulement si $[\mathbb{Q}(S) : F]$ est impair ; comme $2 \notin S$, on a :

$$v_2([\mathbb{Q}(S) : F]) = v_2\Big(\prod_{\ell \in S} (\ell - 1)\Big) - v_2([F : \mathbb{Q}]) .$$

Posons alors (lorsque $p = 2 \in S$, on retrouve (5.5)) :

$$V_2 = v_2\Big(\prod_{\ell \in S} (\ell - 1)\Big) - v_2(2[F : \mathbb{Q}]) \in \{-1, 0\} ; \tag{5.6}$$

on a donc $[\mathbb{Q}(S) : F]$ impair si et seulement si $V_2 = -1$.

D'où l'énoncé final (dont on trouvera une généralisation dans [G5]) :

(5.7) **Théorème.** Soit F un corps abélien imaginaire, soit S l'ensemble des nombres premiers ramifiés dans $F/\mathbb{Q}$, et soit $\rho_F = \sum_{a \in [1,f]'} \Big(-\frac{a}{f} + \frac{1}{2}\Big)\sigma_{a,F}^{-1}$.

Alors on a les résultats suivants :

(i) Si $p \notin S \cup \{2\}$, $v_p(\rho_F) \geq 0$.

(ii) Si $p \in S$ et si F ne contient pas μ_q, on a $v_p(\rho_F) \geq 0$, sauf dans le cas particulier où $p = 2$, F contient un sous-corps imaginaire de $\mathbb{Q}(\mu_{2^\infty})$ mais ne contient pas $\sqrt{-1}$, auquel cas si l'on pose :

$$V_2 = v_2\Big(\prod_{\ell \in S-\{2\}} (\ell - 1)\Big) - v_2([F : F \cap \mathbb{Q}_\infty]) ,$$

on a $v_2(\rho_F) = V_2$ si $V_2 < 0$, $v_2(\rho_F) \geq 0$ sinon.

(iii) Si $p \in S$ et si F contient μ_q, soit

$$V_p = v_p\Big(\prod_{\ell \in S-\{p\}} (\ell - 1)\Big) - v_p(p[F : \mathbb{Q}]) \ ;$$

si $V_p < 0$, alors $v_p(\rho_F) = V_p$, sinon $v_p(\rho_F) \geq 0$.

(iv) Enfin si $p = 2 \notin S$, soit

$$V_2 = v_2\Big(\prod_{\ell \in S} (\ell - 1)\Big) - v_2(2[F : \mathbb{Q}]) \ ;$$

si $V_2 < 0$ (i.e. $V_2 = -1$), alors $v_2(\rho_F) = -1$, sinon $v_2(\rho_F) \geq 0$.

(5.8) **Corollaire.** On a $\rho_F \in \mathbb{Z}[G_F]$ si et seulement si les 2 conditions suivantes sont réalisées :

(i) pour tout $p \in S$ pour lequel F contient μ_q, on a :

$$v_p\Big(\prod_{\ell \in S-\{p\}} (\ell - 1)\Big) - v_p(p[F : \mathbb{Q}]) \ \geq 0;$$

(ii) si $2 \in S$ et si F contient un sous-corps imaginaire de $\mathbb{Q}(\mu_{2^\infty})$ ne contenant pas $\sqrt{-1}$, alors on a :

$$v_2\Big(\prod_{\ell \in S-\{2\}} (\ell - 1)\Big) - v_2([F : F \cap \mathbb{Q}_\infty]) \ \geq 0;$$

(iii) si $2 \notin S$, on a :

$$V_2 = v_2\Big(\prod_{\ell \in S} (\ell - 1)\Big) - v_2(2[F : \mathbb{Q}]) \ \geq 0.$$

(5.9) **Remarque.** (i) On sait que l'on a $\rho_F = (1 - \sigma_{-1,F})\rho_F^+$, où $\rho_F^+ = \sum_{a \in [1, \frac{f}{2}]'} \Big(-\frac{a}{f} + \frac{1}{2}\Big)\sigma_{a,F}^{-1}$. Par conséquent, il n'est pas difficile de vérifier que $v_p(\rho_F^+) = v_p(\rho_F)$ pour tout p.

(ii) Dans le cas particulier $F = \mathbb{Q}$ (où $\rho_F = -\frac{1}{2}$), on a donc $S = \emptyset$ et seul le cas $p = 2 \notin S$ est à considérer, et dans ce cas on a bien comme attendu $V_2 = -v_2(2) = -1$.

(iii) Ainsi, en pratique, les éléments de Stickelberger ρ_F sont le plus souvent entiers ; ceci va permettre une approche différente de la théorie des fonctions L p-adiques (pour certains caractères seulement) en écrivant ces fonctions comme intégrales par rapport à des $\mathbb{Z}_p$-mesures.

6.— Mesures de Stickelberger.

L'étude précédente montre que pour certains corps on va pouvoir définir directement des $\mathbb{Z}_p$-mesures pour l'étude de certaines fonctions L_p.

Soit K un corps abélien imaginaire tel que $K_\infty = K\mathbb{Q}_\infty$ ne contienne pas μ_q ; pour un tel corps, considérons les corps $K_n = K\mathbb{Q}_n$, où $\mathbb{Q}_n$ est le sous-corps de degré p^n, $n \geq 0$, de $\mathbb{Q}_\infty$; alors :

$$\rho_{K_n} \in \mathbb{Z}_p[G_{K_n}], \text{ pour tout } n \geq 0 . \tag{6.1}$$

Soit toujours S_0 l'ensemble des nombres premiers distincts de p ramifiés dans $K/\mathbb{Q}$ et soit $S = S_0 \cup \{p\}$; comme $St_{S,K_n} = \rho_{K_n}$ pour tout $n \geq 1$ (pour $n = 0$, si $K_0 = K$ est de conducteur étranger à p, on obtient $St_{S,K} = (1 - \sigma_{p,K}^{-1})\rho_K$), on constate que

$$St_{S,K_\infty} \in \Lambda_{K_\infty} = \varprojlim_n \mathbb{Z}_p[G_{K_n}] . \tag{6.1.1}$$

(6.2) **Définition.** Soit S un ensemble fini de nombres premiers contenant p. On désigne alors par $M(S)$ une extension imaginaire maximale de $\mathbb{Q}$, contenue dans $\mathbb{Q}(S)$, ayant la propriété suivante : $M(S)$ contient la $\mathbb{Z}_p$-extension cyclotomique $\mathbb{Q}_\infty$ sans contenir le groupe μ_q.
On désigne alors par $St_{M(S)} = St_{S,M(S)}$ les mesures mises en évidence en (6.1.1) et qui sont telles que $St_{M(S),K} = \rho_K$ pour tout $K \subset M(S)$, $K \in \mathcal{F}'_S$, $f \in \mathbb{N}'_S$. On désigne enfin par $St^+_{M(S)}$ une mesure définie modulo $(1+\sigma_{-1,M(S)})\,\Lambda_{M(S)}$, telle que $(1+\sigma_{-1,M(S)})\,St^+_{M(S)} = St_{M(S)}$.

(6.3) **Remarques.** (i) Le choix maximal des $M(S)$ est une simple commodité pour la classification de ces mesures et assure que tout sous-corps imaginaire de $\mathbb{Q}(S)$ contenant $\mathbb{Q}_\infty$ sans contenir μ_q est contenu dans un tel $M(S)$.

(ii) Posons $S_0 = S - \{p\}$; alors les corps $M(S)$ sont ainsi caractérisés :

(α) Si $S_0 = \emptyset$ et si $p = 2$ ou si p est un nombre premier de Fermat (i.e. si $\varphi(q)$ est puissance de 2), alors il n'existe pas de corps $M(S)$.

(β) Si $S_0 = \emptyset$ et si $p \neq 2$ est tel que $p - 1$ n'est pas une puissance de 2, alors les $M(S)$ sont les sous-corps M_ℓ d'indice premier ℓ de $\mathbb{Q}(\{p\})$, pour tout ℓ impair divisant $p - 1$.

(γ) Si $S_0 \neq \emptyset$, les $M(S)$ sont les corps $\mathbb{Q}(S_0)M_\ell$ pour tout diviseur premier ℓ de $\varphi(q)$ (y compris 2).

(iii) On a $St_{M(S)} = \nu_{S,M(S)}\,\delta^{-1}_{M(S)}$, où l'on rappelle que $St_S = \nu_S\,\delta^{-1}$, $\nu_S = \nu_S^\tau \in \Lambda_S$, $\delta = \delta^\tau = 1 - N\tau.\tau^{-1}$, $\tau \in G_S$, $\langle\tau\rangle \neq 1$. Ceci veut dire que sous les hypothèses faites, $\delta_{M(S)}$ divise $\nu_{S,M(S)}$ dans $\Lambda_{M(S)}$.

(6.4) **Remarques.** (i) On voit que ce point de vue ne peut être atteint à partir de la pseudo-mesure DR_S, car la transformée de Mellin m n'est plus définie sur $Gal(M(S)/\mathbb{Q})$ puisque si $\langle\ \rangle$ est un caractère de $M(S)$, ω n'en est plus un, donc N non plus.

(ii) Par exemple, si K est un corps quadratique imaginaire distinct de $\mathbb{Q}(\mu_3)$ pour $p = 3$ et de $\mathbb{Q}(\mu_4)$ pour $p = 2$, il existe un corps $M(S)$ contenant K et par suite $St_{M(S)}$ existe comme mesure.

Abordons maintenant l'aspect fonctions L_p. Soit χ un caractère pair d'ordre fini et soit S l'ensemble de nombres premiers qui lui correspond (S contenant p) ; comme

$$\frac{1}{2}\, L_p(\chi, s) = \langle \omega\chi^{-1}\langle\ \rangle^s,\ St_S^+\rangle \text{ (cf. (1.3.2))},$$

il suffit, pour pouvoir appliquer ce qui précède, que le corps fixe par $\omega^{-1}\chi$ ne contienne pas $\mathbb{Q}(\mu_q)$ ni (pour $p = 2$) de sous-corps imaginaire de $\mathbb{Q}(\{2\})$.

(6.5) **Lemme.** Soit $K_0 = K_{\omega^{-1}\chi}$ le corps fixe par le noyau de $\omega^{-1}\chi$ et posons $\omega^{-1}\chi = \omega^j\psi\chi_r$, où ψ est un caractère de $\mathbb{Q}(S_0)$ et χ_r un caractère de $\mathbb{Q}_\infty$. Alors K_0 ne contient pas $\mathbb{Q}(\mu_q)$ ni (pour $p = 2$) de sous-corps imaginaire de $\mathbb{Q}(\{2\})$ si et seulement si la condition suivante est vérifiée :

on a $(j, o(\omega)) \neq 1$ <u>ou</u> $(o(\psi), o(\omega)) \neq 1$.

Supposons alors cette condition réalisée, et soit $M(S)$ contenant K_0 ; on a alors :

$$\begin{aligned}\frac{1}{2}\, L_p(\chi, s) &= \langle \omega\chi^{-1}\langle\ \rangle^s,\ St^+_{M(S)}\rangle \\ &= \lim_{f\to 0} \langle \omega\chi^{-1}\langle\ \rangle^s, \rho_K^{+\prime}\rangle, K_0 \subseteq K \subset M(S), K \in \mathcal{F}_S',\end{aligned}$$

où $\rho_K^{+\prime}$ prolonge ρ_K^+ dans $\mathbb{Z}_p[G_{M(S)}]$. On peut alors utiliser les corps $K = K_n = K_0\mathbb{Q}_n$, auquel cas on a

$$\rho^+_{K_n} = \sum_{a\in[1,\frac{f_n}{2}]'} \Big(-\frac{a}{f_n} + \frac{1}{2}\Big)\sigma^{-1}_{a,K_n} \mod (1 + \sigma_{-1}, K_n)\mathbb{Z}_p[G_{K_n}]\ ,$$

pour tout $n \geq 1$ ($n \geq 0$ si p est ramifié dans K_0), où f_n est le conducteur de K_n ; écrivons alors dans $\mathbb{Z}_p[G_{K_n}] = \mathbb{Z}_p[G_n]$:

$$\rho^+_{K_n} \equiv \rho_n^+ = \sum_{a\in[1,\frac{f_n}{2}]'} \Big(-\frac{a}{f_n} + \frac{1}{2}\Big)\sigma^{-1}_{a,K_n} = \sum_{\tau_n\in G_n} u_{\tau_n}\ \tau_n^{-1}\ , \tag{6.5.1}$$

et désignons par $\rho_n^{+\prime} = \sum_{\tau_n\in G_n} u_{\tau_n}\ \tau_n'^{-1} \in \mathbb{Z}_p[G_{M(S)}]$ un prolongement arbitraire de ρ_n^+ ; il vient alors :

$$\begin{aligned}\frac{1}{2}\, L_p(\chi, s) &= \lim_{n\to\infty} \langle \omega\chi^{-1}\langle\ \rangle^s,\ \rho_n^{+\prime}\rangle \\ &= \lim_{n\to\infty} \sum_{\tau_n\in G_n} u_{\tau_n}\ \omega^{-1}\chi(\tau_n)\langle\langle\tau_n'\rangle^{-s}\rangle\ .\end{aligned} \tag{6.5.2}$$

(6.6) **Théorème.** Soit χ un caractère pair d'ordre fini de G^{ab} de la forme $\chi = \omega^{1+j}\psi\chi_r$, ψ caractère de $\mathbb{Q}(S_0)$ et χ_r caractère de $\mathbb{Q}_\infty$ avec $(j, o(\omega)) \neq 1$ <u>ou</u> $(o(\psi), o(\omega)) \neq 1$; alors, pour tout $s \in \mathbb{Z}_p$, on a (cf. (6.5.1), (6.5.2)) :

$$\frac{1}{2}\, L_p(\chi, s) \equiv \sum_{\tau_n \in G_n} u_{\tau_n}\, \omega^{-1}\chi(\tau_n)\langle \tau_n' \rangle^{-s} \mod s f_n \mathcal{A}\ ,$$

pour tout $n \geq 0$, où $G_n = Gal(K_n/\mathbb{Q})$, $K_n = K_{\omega^{-1}\chi}\mathbb{Q}_n$ et où f_n est le conducteur de K_n.

démonstration

Il suffit de reprendre le principe utilisé pour la démonstration de (1.5) :

On a

$$\frac{1}{2}\, L_p(\chi, s) - \langle \omega\chi^{-1}\langle\ \rangle^s,\, \rho_n^{+\prime}\rangle = \lim_{\substack{m\to\infty \\ m\geq n}} \langle \omega\chi^{-1}\langle\ \rangle^s,\, \rho_m^{+\prime} - \rho_n^{+\prime}\rangle\ ;$$

comme $\rho_m^{+\prime} - \rho_n^{+\prime}$ est dans l'idéal d'augmentation de $\mathbb{Z}_p[Gal(M(S)/K_n)]$, il suffit d'étudier les quantités

$$\langle \omega\chi^{-1}\langle\ \rangle^s,\, 1 - \sigma'\rangle\ \text{, pour } \sigma' \in Gal(M(S)/K_n)\ .$$

Comme $\omega\chi^{-1}\langle\ \rangle^s$ est un caractère de K_∞, on a $\langle \omega\chi^{-1}\langle\ \rangle^s,\, 1-\sigma'\rangle = 1-\langle\sigma'\rangle^s = 1-\langle\sigma'_{\mathbb{Q}_\infty}\rangle^s$. Posons $K_0 \cap \mathbb{Q}_\infty = \mathbb{Q}_{n_0}$; si $n \geq n_0$, $\sigma'_{\mathbb{Q}_\infty}$ fixe $\mathbb{Q}_n$ et on a, d'après (V.1.4.6), le résultat dans ce cas puisque $f_n \equiv 0 \mod qp^n$ (y compris si $n = 0$, vu l'hypothèse faite) ; si $n < n_0$, $\sigma'_{\mathbb{Q}_\infty}$ fixe $\mathbb{Q}_{n_0}$ et le résultat est encore valable puisque $K_n = K_0 = K_{n_0}$ dans ce cas.

(6.7) **Remarque.** Pour $n < n_0$, où n_0 est l'entier maximum tel que $\mathbb{Q}_{n_0} \subseteq K_0$, on peut donc remplacer le module $sf_n\mathcal{A}$ de la congruence ci-dessus par le module $sf_{n_0}\mathcal{A}$.

C'est sous la forme du théorème (6.6) (lorsque c'est possible) que l'on peut approcher de la façon la plus commode possible les valeurs de $\frac{1}{2}\, L_p(\chi, s)$. On peut alors, pour le calcul des ρ_{K_n} puis de $\frac{1}{2}\, L_p(\chi, s)$ modulo $sf_n\mathcal{A}$, utiliser le logiciel **GALCYCL** mis au point dans [G4].

(6.8) **Exercice.** *On considère le cas particulier d'un corps imaginaire K contenant un sous-corps imaginaire de $\mathbb{Q}(\mu_{2^\infty})$ ne contenant pas $\sqrt{-1}$, et on fixe $p = 2$; on pose :*

$$-t = Min\Big(0, v_2\big(\prod_{\ell\in S-\{2\}} (\ell - 1)\big) - v_2([K : K \cap \mathbb{Q}_\infty])\Big) \qquad (\text{ on a } t \geq 0)\ .$$

Montrer que pour tout $n \geq 0$, $\rho_{K_n} \in \frac{1}{2^t}\, \mathbb{Z}_2[G_{K_n}]$.

Faire l'analogue, pour ce cas particulier, de la théorie détaillée dans ce §6.

Bibliographie

[B] Barsky, D., *Transformation de Cauchy p-adique et algèbre d'Iwasawa*, Math. Ann. 232 (1978), 255–266.

[Bo] Bourbaki, N., *Topologie générale, III, chap.2*, Hermann, Paris (1965).

[B-S] Borevitch, Z.I., Chafarevitch I.R., *Théorie des nombres*, Gauthier-Villars, Paris (1967).

[D-R] Deligne, P., Ribet, K.A., *Values of abelian L-functions at negative integers*, Invent. Math. 59 (1980), 227–286.

[F-G] Ferrero, B., Greenberg, R., *On the behavior of p-adic L-functions at $s = 0$*, Invent. Math. 50 (1978), 91–102.

[F-W] Ferrero, B., Washington, L.C., *The Iwasawa Invariant μ_p vanishes for abelian number fields*, Ann. of Math. 109 (1979), 377–395.

[G1] Gras, G., *Théorie des genres analytique des fonctions L p-adiques des corps totalement réels*, Invent. Math. 86 (1986), 1–17.

[G2] Gras, G., *Pseudo-mesures p-adiques associées aux fonctions L de $\mathbb{Q}$*, Manuscr. Math. 57 (1987), 373–415.

[G3] Gras, G., *Relations congruentielles linéaires entre nombres de classes de corps quadratiques*, Acta Arith. 52 (1989), 147–162.

[G4] Gras, G., *Détermination numérique du groupe d'Artin des extensions cycliques de $\mathbb{Q}$ à ramification donnée (GALCYCL)*, Public. Math. Fac. Sci. Besançon, (Théorie des Nombres) - Années 1984/85 – 1985/86, fasc.2, 34 pp. .

[G5] Gras, G., *Sur les dénominateurs des fonctions zêta partielles*, Public. Math. Fac. Sci. Besançon (Théorie des Nombres) - Années 1991/92 (1993), 15 pp. .

[H] Hasse, H., *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin 1952 (réedition 1985).

[Iw] Iwasawa, K., *Lectures on p-adic L-functions*, Ann. of Math. Studies, Princeton Univ. Press (1972).

[Ko] Koblitz, N., *p-adic number, p-adic analysis, and zeta-functions*, Grad. t. in Math. 58, Springer-Verlag (1977).

[K-L] Kubota, T., Leopoldt, H.W., *Eine p-adische theorie der Zetawerte, I*, J. reine angew. Math., 214/215 (1964), 328–339.

[L] Lang, S., *Cyclotomic fields, I and II (2^{nd} ed.)*, Grad. t. in Math. 121, Springer-Verlag (1990).

[Pi] Pioui, R., *Mesures de Haar p-adiques et interprétation arithmétique de* $\frac{1}{2}L_2(\chi, s) - \frac{1}{2}L_2(\chi, t)$, $s, t \in \mathbb{Z}_2$ *(χ quadratique)*, Thèse (Besançon) 1990.

[Ri] Ribenboim, P., *L'arithmétique des corps*, coll. Méthodes, Hermann, Paris (1972).

[R] Ribet, K.A., *p-adic L-functions attached to characters of p-power order*, Sém. Delange-Pisot-Poitou (Théorie des nombres) 1977/78, n° 9, 8p.

[S1] Serre, J.-P., *Sur le résidu de la fonction zêta p-adique d'un corps de nombres*, C. R. Acad. Sci. Paris 287, Série A (1978), 183–188.

[S2] Serre, J.-P., *Cohomologie galoisienne*, Springer, Lect. N. in Math. 5 (1964).

[S3] Serre, J.-P., *Classes des corps cyclotomiques (d'après Iwasawa)*, Séminaire Bourbaki 174 (1958).

[St] Stark, H.M., *Dirichlet's class number formula revisited, to appear.*

[U1] Urbanowicz, J., *On some new congruences between generalized Bernoulli numbers, I and II*, Publ. Math. Fac. Sci. Besançon (théorie des nombres), Années 1989/90 – 1990/91.

[U2] Urbanowicz, J., *On the 2-primary part of a conjecture of Birch and Tate*, Acta Arith., 43 (1983), 69–81.

[U3] Urbanowicz, J., *Connections between $B_{2,\chi}$ for even quadratic Dirichlet character χ and class numbers of appropriate imaginary quadratic fields, I*, Compositio Math. 75 (1990), 247–270.

[W] Washington, L.C., *Introduction to cyclotomic fields*, Grad. t. in Math. 83, Springer-Verlag (1982).

Index des principales notations

p	nombre premier
q	p si $p \neq 2, 4$ sinon
v_p	valuation de $\mathbb{Q}_p$
$(x)_p$	$p^{v_p(x)}$
$(x)^*$	$xp^{-v_p(x)}$
φ	indicateur d'Euler
$o(\ )$	ordre d'un élément d'un groupe
G, H	groupe profini commutatif, sous-groupe fermé de G
$G(p)$	p-Sylow de G
Γ	sous-groupe de G isomorphe à $\mathbb{Z}_p$
γ, T	générateur topologique de Γ, $1-\gamma$
Ω_G	ensemble des sous-groupes ouverts de G
$\mathcal{C}_G$	ensemble des classes de G-modulo les éléments de Ω_G
$\mathcal{U}_G$	ensembles des ouverts compacts de G
$\mathcal{M}_G$	algèbre des $\mathbb{Z}_p$-mesures sur G
Λ_G	$\varprojlim_{H \in \Omega_G} \mathbb{Z}_p[G/H] \simeq \mathcal{M}_G$
λ, μ, ν	$\mathbb{Z}_p$-mesures
α_G	$\mathbb{Z}_p$-mesure de Haar sur G ($G(p)$ fini)
$\widetilde{\Lambda}_G$	ensemble des $\mathbb{Z}_p$-pseudo-mesures sur G
$\langle f, \mu \rangle$	intégrale de f sur G pour la mesure μ
X_G	groupe des caractères continus de G
$tor(X_G)$	éléments d'ordre fini de X_G
Φ	transformée de Fourier
Δ_G, Δ_G'	algèbre des $\mathbb{Z}_p$-distributions sur G, sous-algèbre formée des $\rho = \frac{\nu}{\delta} \in \Delta_G$, δ_H non nul et non diviseur de 0 dans $\mathbb{Z}_p$[G/H], pour tout $H \in \Omega_G$
$\mathbb{P}$	ensemble des nombres premiers
S	partie finie de $\mathbb{P}$ (en général contenant p)
S_0	$S - \{p\}$
$\mathbb{N}_S$	sous-monoïde multiplicatif de $\mathbb{N} - \{0\}$ engendré par S
$\mathbb{N}_S'$	sous-ensemble de $\mathbb{N}_S$ formé des m divisibles par tous les éléments de S
$\mathbb{Q}^{ab}$	extension abélienne maximale de $\mathbb{Q}$ dans $\mathbb{C}_p$
$\mathbb{Q}(S)$, $\mathbb{Q}(\{p\})$	extension abélienne maximale de $\mathbb{Q}$ dans $\mathbb{C}_p$ non ramifiée en dehors de $S \cup \{\infty\}$, $\mathbb{Q}(S)$ pour $S = \{p\}$
$\mathbb{Q}(f)$, $\mathbb{Q}(f)^+$	corps cyclotomique des racines f-ièmes de l'unité, sous-corps réel maximal
$\mathbb{Q}_\infty$, $\mathbb{Q}_r$	$\mathbb{Z}_p$ extension cyclotomique de $\mathbb{Q}$, sous-corps de $\mathbb{Q}_\infty$ de degré p^r
F, G_F	sous-corps de $\mathbb{Q}^{ab}$ ou $\mathbb{Q}(S)$ de degré fini, $Gal(F/\mathbb{Q})$
$\mathcal{F}_S$	ensemble des sous-corps de degré fini de $\mathbb{Q}(S)$
$\mathcal{F}_S'$	$\{F \in \mathcal{F}_S,\ F \notin \mathcal{F}_U$ pour tout $U \underset{\neq}{\subset} S\}$

G_S, $G_S(p)$	$Gal(\mathbb{Q}(S)/\mathbb{Q})$, p-Sylow de G_S
A_S, B_S	$Gal(\mathbb{Q}(S)/\mathbb{Q}_\infty)$, $Gal(\mathbb{Q}(S)/\mathbb{Q}(\{p\}))$
Γ, H_ℓ	$Gal(\mathbb{Q}(S)/\mathbb{Q}(S_0)\mathbb{Q}(q))$, $Gal(\mathbb{Q}(S)/\mathbb{Q}(S-\{\ell\}))$
σ_a, $(a,S)=1$	symbole d'Artin sur $\mathbb{Q}(S)$
$\sigma_{a,F}$	restriction de σ_a à $F \subseteq \mathbb{Q}(S)$
σ_{-1}	conjugaison complexe
X^{ab}	groupe des caractères continus $G^{ab} \to \mathbb{C}_p$
$tor(X^{ab})$	sous-groupe des caractères d'ordre fini
Λ_S, $\widetilde{\Lambda}_S$	Λ_{G_S}, $\widetilde{\Lambda}_{G_S}$
Δ_S, Δ'_S	Δ_{G_S}, Δ_{G_S}
α_{A_S}, α_{B_S}	$\mathbb{Z}_p$-mesure de Haar sur A_S, B_S
ρ_F	élément de Stickelberger de F
St_S, St_S^+	distribution de Stickelberger sur G_S, on a $(1-\sigma_{-1})St_S^+ = St_S$
DR_S, DR_S^-	pseudo-mesure de Deligne-Ribet sur G_S, on a $(1+\sigma_{-1})DR_S^- = DR_S$
m	involution de Mellin sur Δ_S
χ, ψ	éléments de $tor(X^{ab})$ (caractères d'ordre fini)
χ_r	caractère d'ordre p^r de $\mathbb{Q}_r \subset \mathbb{Q}_\infty$
χ_0	caractère unité
K_χ	sous-corps de $\mathbb{Q}^{ab}$ fixe par $Ker(\chi)$
ω	caractère de Teichmüller (caractère de $\mathbb{Q}(q)$) défini par la projection $G_S \to tor(\mathbb{Z}_p^*)$
$\langle\ \rangle$	caractère de $\mathbb{Q}_\infty$ défini par la projection $G_S \to 1+q\mathbb{Z}_p$
N	$\omega\langle\ \rangle$
$\mathbb{Z}_p(\chi)$	anneau des valeurs de χ sur $\mathbb{Z}_p$
v_χ	valuation normalisée sur $\mathbb{Z}_p(\chi)$
f, f_χ	conducteur de F, du caractère χ (i.e. de K_χ)
$[1,f]'$	$=\{a \in \mathbb{N},\ 1 \le a \le f,\ (a,f)=1\}$
$[1,\frac{f}{2}]'$	$=\{a \in \mathbb{N},\ 1 \le a \le \frac{f}{2},\ (a,f)=1\}$
r_a^c	$=\frac{1}{f}([\frac{a}{c}]_f c - a)$, où $[u]_f$ est le représentant entier modulo f de $u \in \mathbb{Q}^\times$ dans $[1,f]'$, pour a,c étrangers à f
R_a^c	$r_a^c + \frac{1-c}{2}$
$B_n(\chi)$, B_n	nombres de Bernoulli généralisés, $B_n(\chi_0)$ (nombres de Bernoulli ordinaires)
$\mathbb{B}_n(X)$	polynomes de Bernoulli
$\frac{1}{2}L_p(\chi,s)$	$\langle \omega\chi^{-1}\langle\ \rangle^s, St_S^+\rangle = \langle \chi\langle\ \rangle^{1-s}, DR_S^-\rangle$
λ_ψ, μ_ψ	invariants d'Iwasawa analytiques de ψ
$\mathbb{C}_p$	complété d'une clôture algébrique de $\mathbb{Q}_p$
$\mathcal{O}_p$, $\mathcal{M}_p$	anneau des entiers, idéal maximal de $\mathbb{C}_p$
$\mathcal{O}_p^*$, $\mathcal{U}_p$	groupe des unités, $1+\mathcal{M}_p$
$\mathcal{A}$, $\mathcal{A}^*$	algèbre d'Iwasawa, groupe des éléments inversibles de $\mathcal{A}$
μ_n, μ_{p^∞}	groupe des racines n-ièmes de l'unité dans $\mathbb{C}_p$, $\cup_{n\ge 0}\mu_{p^n}$